

Программный комплекс
«Система мониторинга и управления
событиями безопасности
Ankey SIEM Next Generation» v 5.2.3

Руководство по инсталляции
Часть 1.

Инсталляция ПК Ankey SIEM NG в
исполнениях

Ankey SIEM NG и

Ankey SIEM NG с дополнительным компонентом VM

© ООО «Газинформсервис» с 2004 года

При инсталляции ПК Ankey SIEM NG необходимо ознакомиться с условиями лицензионного соглашения на использование конечным пользователем программы*, согласно которому весь функционал программного комплекса, в том числе отдельные его модули (составляющие)**, носители и документация, предоставляются на условиях «как есть»***.

Этот документ входит в комплект поставки программного обеспечения, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения ООО «Газинформсервис».

Ankey SIEM NG ® является зарегистрированным товарным знаком ООО «Газинформсервис».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

За содержание, качество, актуальность и достоверность используемых в документе материалов, права на которые принадлежат другим правообладателям, а также за возможный ущерб, связанный с использованием этих материалов, ООО «Газинформсервис» ответственности не несет.

Дата редакции документа: 4 квартал 2024 года.

* Использование ПК Ankey SIEM NG означает согласие со всеми пунктами лицензионного соглашения.

** ПК Ankey SIEM NG включает в свой состав компоненты платформы, коннекторы (модули сбора и обработки данных) и контент (модули выявления нарушений ИБ (корреляционной обработки данных)).

*** Выполнение основных функций программы (функциональные возможности), предусмотренных (-е) действующей релизной версией. Комплектность, предусмотренная действующей релизной версией изделия. Документация, предусмотренная действующей релизной версией изделия.

Содержание

1 Об этом документе	7
2 О ПК Ankey SIEM NG	11
2.1 Архитектура ПК Ankey SIEM NG	13
2.1.1 Компонент Ankey SIEM Next Generation Core	13
2.1.2 Компонент Ankey SIEM Next Generation Server	13
2.1.3 Компонент Ankey SIEM Next Generation Events Storage	13
2.1.4 Компонент Ankey SIEM Next Generation Collector	13
2.1.5 Компонент Ankey SIEM Next Generation Management and Configuration	14
2.1.6 Компонент Ankey SIEM Next Generation Knowledge Base	14
2.1.7 Компонент Ankey SIEM Next Generation Retro Correlator	15
2.2 Схема взаимодействия компонентов	15
3 Развертывание ПК Ankey SIEM NG	21
3.1 Типовые схемы развертывания ПК Ankey SIEM NG	21
3.1.1 Рекомендации по выбору конфигурации ПК Ankey SIEM NG	21
3.1.2 Схема развертывания конфигурации для низконагруженных систем	22
3.1.3 Схема развертывания конфигурации для средненагруженных систем	26
3.1.4 Схема развертывания конфигураций для высоконагруженных систем	30
3.1.5 Схемы масштабирования Ankey SIEM NG	34
3.2 Аппаратные и программные требования	39
3.2.1 Требования к программному обеспечению и среде установки	39
3.2.2 Требования к аппаратному обеспечению конфигурации для низконагруженных систем	43
3.2.3 Требования к аппаратному обеспечению конфигурации для средненагруженных систем	46
3.2.4 Требования к аппаратному обеспечению конфигурации для высоконагруженных систем	50
3.2.5 Аппаратные требования к серверу сбора событий с компонентом Ankey SIEM NG Collector, размещенному в отдельном сегменте сети	56
3.2.6 Аппаратные требования к серверу облегченной версии Ankey SIEM NG Server («SIEM на коллекторе»)	58
3.2.7 Рекомендации по расчету объема и выбору накопителей для хранения событий	59
3.2.8 Рекомендации по развертыванию ПК Ankey SIEM NG в виртуальной среде	60
3.2.9 Взаимодействие с внешними системами	62
3.3 Подготовка к развертыванию Ankey SIEM NG	62
3.4 Об установке компонентов на Linux с помощью ролей	63
3.5 Сценарий развертывания ПК Ankey SIEM NG	66
3.6 Установка роли Deployer	68
3.7 Установка компонента Ankey SIEM NG MC	69

3.7.1 Установка модуля Salt Minion на сервер Ankey SIEM NG Core	70
3.7.2 Установка роли SqlStorage	71
3.7.3 Установка роли JatobaStorage и онлайн активация лицензии.....	72
3.7.4 Установка роли JatobaStorage и офлайн активация лицензии.....	73
3.7.5 Установка роли Management and Configuration.....	75
3.8 Установка компонента Knowledge Base	78
3.9 Установка компонента Ankey SIEM NG Core	79
3.9.1 Установка роли RMQ Message Bus на сервер Ankey SIEM NG Core ...	79
3.9.2 Установка роли Core	80
3.10 Установка компонента Ankey SIEM NG Events Storage	81
3.10.1 Установка модуля Salt Minion на сервер Ankey SIEM NG Events Storage	82
3.10.2 Установка роли SIEM Storage с хранилищем событий Elasticsearch .	83
3.10.3 Установка роли SIEM Storage с хранилищем событий LogSpace	86
3.11 Установка компонента Ankey SIEM NG Server	87
3.11.1 Установка модуля Salt Minion на сервер Ankey SIEM NG Server.....	88
3.11.2 Установка роли RMQ Message Bus на сервер Ankey SIEM NG Server	89
3.11.3 Установка роли SIEM Server	90
3.12 Активация лицензии ПК Ankey SIEM NG	92
3.12.1 Активация лицензии на Linux при наличии доступа к интернету.....	92
3.12.2 Активация лицензии на Linux при отсутствии доступа к интернету ...	93
3.13 Удаление лицензионного ключа.....	94
3.14 Установка стандартной базы данных, стандартных модулей сбора и обработки	94
3.14.1 Создание корневой базы данных GIS_DB	95
3.14.2 Установка актуальной таксономии	95
3.14.3 Импорт пакета стандартных коннекторов и контента	96
3.14.4 Импорт пакета стандартного контента	97
3.14.5 Создание ветки Customer Data	99
3.14.6 Установка SDK	101
3.14.7 Установка ресурсов в Ankey SIEM NG Server	101
3.15 Установка компонента Ankey SIEM NG Collector.....	104
3.15.1 Установка модуля Salt Minion на сервер Ankey SIEM NG Collector ..	105
3.15.2 Установка роли Collector	106
3.16 Установка компонента Ankey SIEM NG Collector на Microsoft Windows.....	107
3.17 Установка облегченной версии компонента Ankey SIEM NG Server на Linux	109
3.17.1 Установка модуля Salt Minion на сервер облегченной версии Ankey SIEM NG Server	109
3.17.2 Установка роли RMQ Message Bus на сервер облегченной версии Ankey SIEM NG Server	110
3.17.3 Установка роли SIEM Server для облегченной версии компонента .	112
3.18 Установка облегченной версии компонента Ankey SIEM NG Server на	

Microsoft Windows	113
3.19 Установка правил нормализации и агрегации для облегченной версии Ankey SIEM NG Server.....	114
3.20 Установка дополнительного компонента Ankey SIEM NG RC.....	114
3.20.1 Установка модуля Salt Minion на сервер Ankey SIEM NG RC	115
3.20.2 Установка роли RMQ Message Bus на сервер Ankey SIEM NG RC ..	116
3.20.3 Установка роли Retro Correlator	117
3.21 Установка доверенного сертификата для сайта ПК Ankey SIEM NG	118
3.22 Установка пользовательского сертификата для RMQ Message Bus и компонентов Ankey SIEM NG Core, Ankey SIEM NG Server и Ankey SIEM NG Collector	119
3.23 Настройка обновления экспертных данных.....	121
3.23.1 Схемы получения обновлений экспертных данных, поддерживаемые Ankey SIEM NG.....	122
3.23.2 Удаление компонента UCS	127
3.23.3 Изменение параметров обновления экспертных данных для роли Management and Configuration.....	127
3.23.4 Аппаратные и программные требования к локальному серверу обновлений.....	129
3.23.5 Установка локального сервера обновлений	129
3.23.6 Активация лицензии локального сервера обновлений	130
3.23.7 Настройка подключения локального сервера обновлений к прокси- серверу	131
3.23.8 Настройка автоматического переноса обновлений в закрытый сегмент сети	132
3.23.9 Ручной перенос обновлений Ankey SIEM NG в закрытый сегмент сети	134
3.23.10 Проверка и изменение параметров локального сервера обновлений	134
3.24 Настройка ПК Ankey SIEM NG для обеспечения его безопасной работы.136	
3.24.1 Настройка ПК Ankey SIEM NG в конфигурации для низконагруженных систем	136
3.24.2 Настройка ПК Ankey SIEM NG в конфигурации для средненагруженных систем	140
3.24.3 Настройка ПК Ankey SIEM NG в конфигурации для высоконагруженных систем	145
4 Обновление ПК Ankey SIEM NG	151
4.1 Обновление с помощью дистрибутивов	151
4.1.1 Обновление роли Deployer.....	152
4.1.2 Обновление компонента Ankey SIEM NG MC на Linux	153
4.1.3 Обновление компонента Knowledge Base на Linux	157
4.1.4 Обновление компонента Ankey SIEM NG Core на Linux	158
4.1.5 Обновление версии 4.0 компонента Ankey SIEM NG Events Storage на Linux	159

4.1.6 Обновление версии 4.0 компонента Ankey SIEM NG Server на Linux	162
4.1.7 Обновление облегченной версии компонента Ankey SIEM NG Server на Linux	164
4.1.8 Обновление облегченной версии компонента Ankey SIEM NG Server на Microsoft Windows.....	166
4.1.9 Обновление правил нормализации и агрегации для облегченной версии Ankey SIEM NG Server	167
4.1.10 Обновление компонента Ankey SIEM NG Collector на Linux	168
4.1.11 Обновление компонента Ankey SIEM NG Collector на Microsoft Windows	169
4.1.12 Обновление версии 4.0 компонента Ankey SIEM NG RC	170
5 Удаление компонентов из ОС Windows	172
6 Диагностика и решение проблем	173
Перечень сокращений.....	174
Приложение А Порядок установки ПК Ankey SIEM NG.....	178
Приложение Б Параметры конфигурации компонентов ПК Ankey SIEM NG на Linux.....	181
Приложение В Параметры конфигурации компонентов ПК Ankey SIEM NG на Microsoft Windows	203
Приложение Г Рекомендуемые конфигурации для систем хранения событий информационной безопасности	212
Приложение Д Установка модулей сбора и обработки данных и модули выявления нарушений ИБ (корреляционной обработки данных)	213
Д.1 Установка дополнительных модулей сбора и обработки данных	213
Д.2 Установка дополнительных модулей выявления нарушений ИБ (корреляционной обработки данных).....	214
Д.2.1 Иерархия пакетов контента	215
Д.2.2 Установка и удаление дополнительного пакета контента в ПК Ankey SIEM NG.....	216
Д.2.3 Работа с ресурсами в пользовательской ветке Customer_Data	222
Приложение Е Применение патчей в ПК Ankey SIEM NG (5.2.3).....	224

1 Об этом документе

Руководство по инсталляции содержит информацию для планирования и выполнения развертывания программного комплекса Ankey SIEM Next Generation в вариантах исполнения Ankey SIEM NG и Ankey SIEM NG с дополнительным компонентом VM.

Настройка и установка ПК Ankey SIEM NG (далее также – Система) в обозначенных выше вариантах исполнения идентична. Для обозначенных выше вариантов исполнения в документе используется наименование ПК Ankey SIEM NG.

Настройки, специфичные для развертывания варианта исполнения Ankey SIEM NG или Ankey SIEM NG выделены по тексту в виде примечаний и дополнений.

Примечание. Описание вариантов исполнения ПК Ankey SIEM NG и их функций приведено в документе «Руководство администратора Ankey SIEM NG 5.2.3».

В руководстве вы найдете типовые схемы развертывания ПК Ankey SIEM NG, а также инструкции по установке, первоначальной настройке, обновлению и удалению продукта.

Руководство адресовано руководителям и специалистам ИТ-подразделения организации, которые планируют и выполняют развертывание ПК Ankey SIEM NG.

Комплект документации ПК Ankey SIEM NG включает в себя документы, представленные в таблице 1.1.

Таблица 1.1 – Комплект документации ПК Ankey SIEM NG

Каталог	Наименование документа	Описание
Сведения о релизе	Обзор новых возможностей Ankey SIEM NG	Содержит описание изменений между выпускаемой и предыдущей версиями ПК Ankey SIEM NG
	Актуальные версии прикладных модулей ПК Ankey SIEM NG	Содержит список актуальных версий сборок всех поддерживаемых ресурсов к ПК Ankey SIEM NG, разработанных ООО "Газинформсервис"
Основное	Руководство администратора Ankey SIEM NG	Содержит справочную информацию о ПК Ankey SIEM NG и вариантах его исполнения, а также инструкции по настройке и администрированию продукта
	Руководство оператора Ankey SIEM NG	Содержит сценарии использования продукта для управления информационными активами организации и событиями информационной безопасности

Каталог	Наименование документа	Описание
	Руководство по настройке Ankey SIEM NG Event Broker	Содержит справочную информацию и инструкции по настройке и администрированию компонента Event Broker
Инсталляция	Руководство по инсталляции Часть 1. Инсталляция ПК Ankey SIEM NG в исполнениях Ankey SIEM NG и Ankey SIEM NG с дополнительным компонентом VM	Содержит информацию для внедрения вариантов исполнения Ankey SIEM NG и Ankey SIEM NG с дополнительным компонентом VM в инфраструктуре организации: от типовых схем развертывания до инструкций по установке, первоначальной настройке, обновлению и удалению продукта
	Руководство по инсталляции Часть 2. Инсталляция ПК Ankey SIEM NG в исполнении Ankey SIEM NG VM	Содержит информацию для внедрения варианта исполнения Ankey SIEM NG VM в инфраструктуре организации: от типовых схем развертывания до инструкций по установке, первоначальной настройке, обновлению и удалению продукта
Подключение инфраструктуры	Руководство по настройке аудита активов Ankey SIEM NG (AM+VM+HCC)	Содержит рекомендации по интеграции элементов ИТ-инфраструктуры организации с ПК Ankey SIEM NG для аудита активов
	Руководство по интеграции с источниками событий Ankey SIEM NG.	Содержит рекомендации по интеграции элементов ИТ-инфраструктуры организации с ПК Ankey SIEM NG для сбора событий с источников
	Руководство по интеграции с источниками событий Ankey SIEM NG. Приложение А	Содержит перечни регистрируемых событий, маппинг событий и результаты обработки для поддерживаемых источников пакета стандартных коннекторов ПК Ankey SIEM NG
	Руководство по интеграции с источниками событий Ankey SIEM NG. Список изменений	Содержит список изменений пакета стандартных коннекторов ПК Ankey SIEM NG
Настройка корреляции	Пакет общих ресурсов контента. Описание пакета экспертизы <Номер версии пакета>.	Содержит справочную информацию и инструкции по установке и настройке пакета общих ресурсов контента ПК Ankey SIEM NG
	Пакет общих ресурсов контента Приложение А <Номер версии пакета>.	Содержит списки применимых правил корреляции из состава пакета общих ресурсов контента ПК Ankey SIEM NG для поддерживаемых источников

Каталог	Наименование документа	Описание
	Пакет общих ресурсов контента Список изменений <Номер версии пакета>	Содержит список изменений пакета общих ресурсов контента ПК Ankey SIEM NG
	Пакет мониторинга SIEM Описание пакета экспертизы <Номер версии пакета>	Содержит списки применимых правил корреляции из состава пакета мониторинга SIEM для ПК Ankey SIEM NG
	Пакет мониторинга SIEM Список изменений <Номер версии пакета>	Содержит список изменений пакета мониторинга SIEM к ПК Ankey SIEM NG
Инструкции к разработке	Руководство разработчика Ankey SIEM NG	Содержит рекомендации по созданию правил нормализации, корреляции, агрегации и обогащения событий, описание утилит Ankey SIEM NG SDK для их отладки, а также информацию о доступных в ПК Ankey SIEM NG функциях сервиса REST API
	Синтаксис языка запроса PDQL	Содержит справочную информацию и примеры синтаксиса, основных функций и операторов языка PDQL, используемых при работе с ПК Ankey SIEM NG
	PDQL-запросы для анализа активов	Содержит информацию о стандартных запросах на языке PDQL, предназначенных для проверки конфигураций активов при работе в ПК Ankey SIEM NG
Дополнительно	Инструкция по обновлению Ankey SIEM NG с версии 4.x на версию 5.x	Содержит шаги, необходимые для обновления ПК Ankey SIEM NG с версии 4.1 до версии 5.2
	Инструкция по установке и настройке Ankey Update Mirror	Содержит информацию об установке и настройке локального сервера обновлений для получения обновлений экспертных данных компонента Ankey SIEM NG VM
	Инструкция по обновлению пакетов ресурсов с версии 3.x.x на версию 4.x.x	Содержит информацию, необходимую для обновления пакетов ресурсов ПК Ankey SIEM NG с версии 3.x.x на версию 4.x.x

В документе приняты условные обозначения.

Таблица 1.2 – Условные обозначения

Пример текста с условным обозначением	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
❖ Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите кнопку ОК	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду <code>Stop-Service</code>	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
<code>Ctrl+Alt+Delete</code>	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

2 О ПК Ankey SIEM NG

Ankey SIEM Next Generation – это система управления событиями и информацией о безопасности, которая предназначена для сбора, хранения и анализа данных о событиях, которые генерируют различные источники в ИТ-инфраструктуре организаций. ПК Ankey SIEM NG позволяет обеспечивать мониторинг информационной безопасности как всей инфраструктуры, так и отдельных подразделений, узлов и приложений.

ПК Ankey SIEM NG предоставляет следующие основные возможности:

- **Инвентаризация активов.** Система регулярно собирает данные о сетевых узлах и связях между ними;
- **Сбор данных о событиях.** Система собирает данные о событиях с источников событий. В качестве источника событий может выступать любое поддерживаемое оборудование или ПО;
- **Анализ событий для выявления инцидентов ИБ.** Набор специальных правил, на основе которых выполняется анализ;
- **Управление инцидентами ИБ.** Система помогает организовать работу по расследованию инцидентов информационной безопасности и устранению их последствий;
- **Визуализация данных.** Сводная информация об активах, событиях и инцидентах отображается в веб-интерфейсе системы в виде диаграмм и таблиц.
- **Пакеты экспертизы.** Использование базы знаний, разработанной экспертами ООО «Газинформсервис». База содержит данные о самых современных тактиках и техниках хакерских атак и помогает выявлять даже сложные нетиповые атаки;
- **Автоматизация работы с активами.** Система может автоматически устанавливать значимость активов и сроки актуальности данных об активах, полученных в результате сканирования ИТ-инфраструктуры;
- **Повторная проверка событий.** Ретроспективная корреляция полученных ранее событий после добавления новых правил или обновления данных табличных списков; ретроспективный поиск индикаторов компрометации;
- **Отправка уведомлений.** Оповещение ответственных об изменениях в ИТ-инфраструктурах организаций, о работе задач сбора данных Ankey SIEM NG, собираемых событиях, а также о выявляемых инцидентах ИБ.

При активации дополнительного компонента VM с помощью лицензии обеспечивается выполнение следующих функций:

- **Информация об уязвимостях на активах.** На основе постоянно обновляемой базы знаний Ankey SIEM NG предоставляет пользователю и другим системам актуальную информацию об уязвимостях, обнаруженных

на активах. Ankey SIEM NG определяет способы устранения уязвимостей и позволяет настраивать политики контроля.

- **Оценка уязвимостей на активах.** Система выбирает среди уязвимостей те, которые необходимо устранять в первую очередь, и отображает степень защищенности активов.

При активации дополнительного модуля Host Compliance Control (далее также – НСС) с помощью лицензии обеспечивается выполнение следующих функций:

- **Сбор информации о параметрах безопасности.** Дополнительный модуль НСС получает полную информацию о составе ИТ-инфраструктуры и собирает сведения о параметрах безопасности.
- **Оценка соответствия стандартам безопасности.** Дополнительный модуль НСС отслеживает соответствие ИТ-инфраструктуры готовым стандартам, отдельным требованиям и может приоритезировать обнаруженные риски;

2.1 Архитектура ПК Ankey SIEM NG

Ankey SIEM NG состоит из программных компонентов, которые вы можете размещать как на одном сервере, так и на нескольких. Гибкая архитектура позволяет масштабировать и внедрять ПК Ankey SIEM NG в организации с ИТ-инфраструктурами разных масштабов. Если поток событий в ПК Ankey SIEM NG превышает 5000¹ событий в секунду, то требуется распределенная установка компонентов ПК Ankey SIEM NG.

2.1.1 Компонент Ankey SIEM Next Generation Core

Компонент Ankey SIEM Next Generation Core (далее – Ankey SIEM NG Core) является основным компонентом системы, ее управляющим сервером. Ankey SIEM NG Core устанавливается в центральном офисе компании или в крупных территориальных и функциональных подразделениях и выполняет следующие функции:

- централизованное хранение конфигурации активов;
- централизованное управление всеми компонентами системы;
- оперативное реагирование на инциденты информационной безопасности;
- обеспечение взаимодействия подразделений организации при расследовании инцидентов;
- автоматизацию процесса управления уязвимостями²;
- поддержку веб-интерфейса системы.

2.1.2 Компонент Ankey SIEM Next Generation Server

Компонент Ankey SIEM Next Generation Server (далее – Ankey SIEM NG Server) выполняет основные функции по обработке событий безопасности:

- нормализацию, агрегацию, обогащение и корреляцию событий;
- автоматическое создание инцидентов;
- создание активов из событий;
- привязку событий к активам.

2.1.3 Компонент Ankey SIEM Next Generation Events Storage

Компонент Ankey SIEM Next Generation Events Storage (далее – Ankey SIEM NG Events Storage) обеспечивает централизованное хранение информации о событиях безопасности.

2.1.4 Компонент Ankey SIEM Next Generation Collector

Компонент Ankey SIEM Next Generation Collector (далее – Ankey SIEM NG Collector) сканирует активы ИТ-инфраструктуры организации и собирает события с источников. Ankey SIEM NG Collector имеет модульную структуру. Модули сканирования позволяют обнаруживать узлы и их открытые сетевые сервисы и

¹ более 5 000 событий в секунду при использовании модуля syslog, более 3 000 событий в секунду при смешанном сборе событий.

² в исполнении Ankey SIEM NG с дополнительным компонентом VM.

проводить специализированные проверки в режиме теста на проникновение.

Ankey SIEM NG Collector собирает следующую информацию об активах:

- название;
- версию и производителя операционной системы;
- установленные обновления ОС;
- список установленного ПО;
- параметры ОС и ПО;
- учетные записи пользователей и их привилегии;
- данные об аппаратном обеспечении, запущенных сетевых сервисах и службах ОС;
- параметрах сети и средств защиты.

Ankey SIEM NG Collector управляет модулями и обеспечивает мониторинг их состояния, а также передачу данных между модулями и компонентом Ankey SIEM NG Server.

К одному компоненту Ankey SIEM NG Server можно подключать несколько компонентов Ankey SIEM NG Collector. Это позволяет увеличивать производительность, учитывать при сканировании топологию сети и типы каналов связи (например, наличие межсетевых экранов или других средств защиты).

2.1.5 Компонент Ankey SIEM Next Generation Management and Configuration

Компонент Ankey SIEM Next Generation Management and Configuration (далее – Ankey SIEM NG Management and Configuration или Ankey SIEM NG MC) обеспечивает:

- сервис единого входа в продукты ПК Ankey SIEM NG, развернутые в инфраструктуре организации;
- управление пользователями системы, включая создание учетных записей, назначение прав, блокирование и активацию учетных записей;
- интеграцию с Microsoft Active Directory, включая аутентификацию пользователей и синхронизацию прав доступа;
- управление иерархией продуктов ПК Ankey SIEM NG;
- журналирование действий пользователей;
- сведения об уязвимостях (об условиях их возникновения и способах устранения) и бюллетенях безопасности³.

2.1.6 Компонент Ankey SIEM Next Generation Knowledge Base

Компонент Ankey SIEM Next Generation Knowledge Base (далее – Ankey SIEM NG Knowledge Base) – это единая база знаний ПК, которая содержит схему полей событий, пакеты экспертизы (наборы правил и табличных списков), макросы (фильтры), а также сведения о возможном ПО на активах. Вместе с Ankey SIEM NG Knowledge Base устанавливаются утилиты (Software Development Kit или SDK) для разработки правил, макросов, табличных списков,

³ в исполнении Ankey SIEM NG с дополнительным компонентом VM

валидации и управления установочными базами данных.

Создание, редактирование и хранение пакетов экспертизы и табличных списков для последующей установки в компонент Ankey SIEM NG Server осуществляется в приложении Ankey SIEM NG Knowledge Base.

Примечание. Описание дополнительных модулей сбора и обработки данных и модули выявления нарушений ИБ (корреляционной обработки данных) представлено в приложении Д.

2.1.7 Компонент Ankey SIEM Next Generation Retro Correlator

Компонент Ankey SIEM Next Generation Retro Correlator (далее также – Ankey SIEM NG Retro Correlator или Ankey SIEM NG RC) выполняет повторную проверку полученных ранее событий при помощи правил корреляции. В состав компонента входят службы agent.service и siemserver-retrocontroller.service.

2.2 Схема взаимодействия компонентов

Взаимодействие компонентов ПК Ankey SIEM NG отражено на рисунке 1.1.

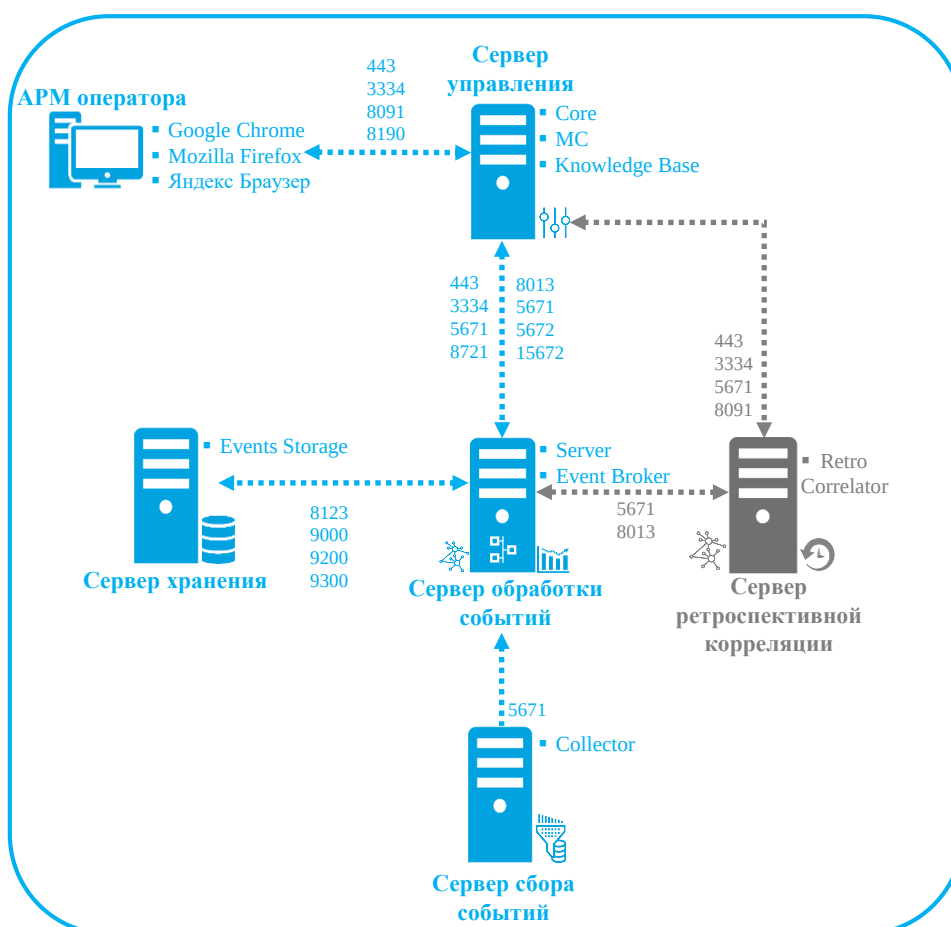


Рисунок 1.1 – Схема взаимодействия компонентов ПК Ankey SIEM NG в варианте исполнения Ankey SIEM NG

Взаимодействие компонентов ПК Ankey SIEM NG с дополнительным компонентом VM отражено на рисунке 1.2.

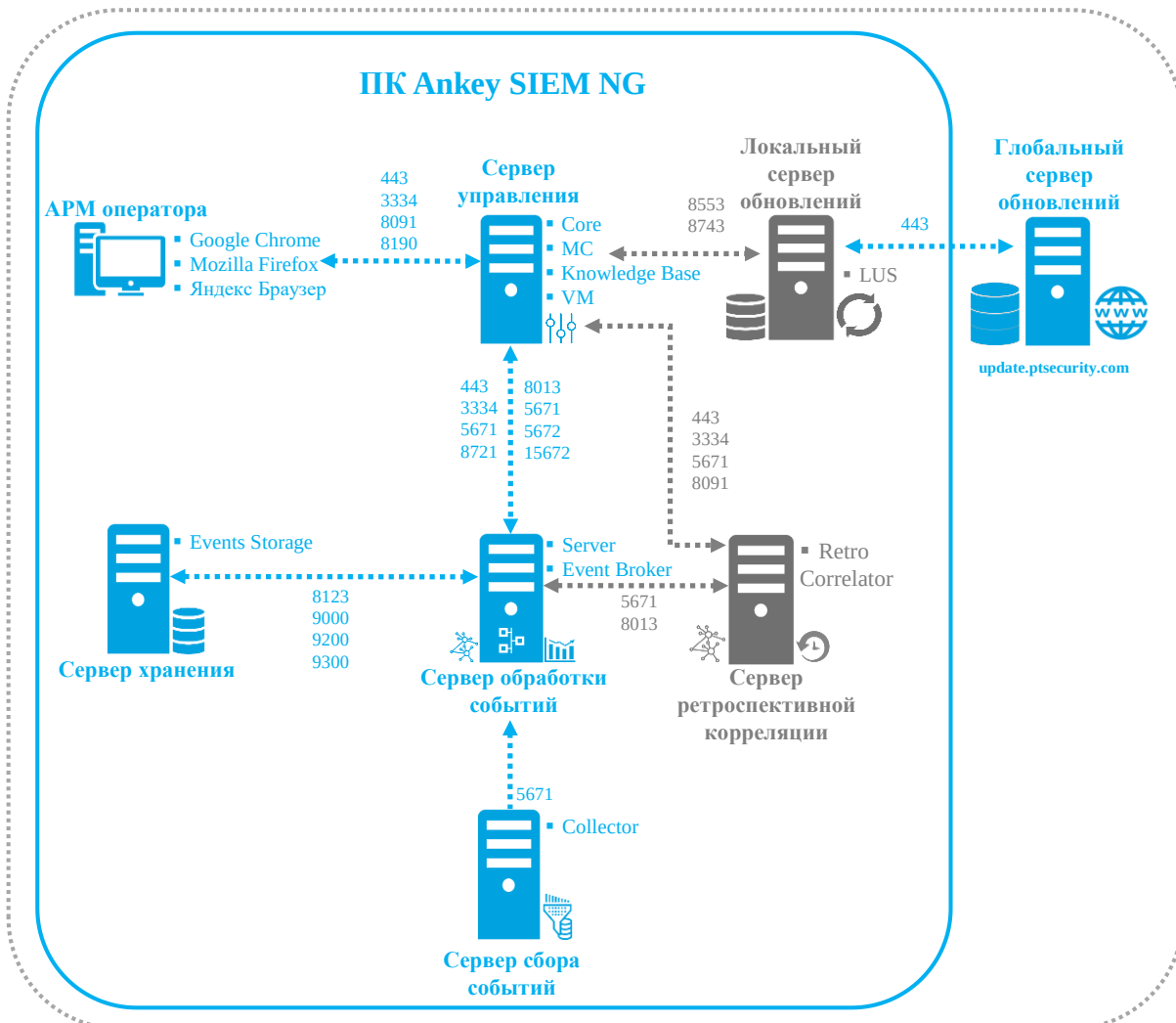
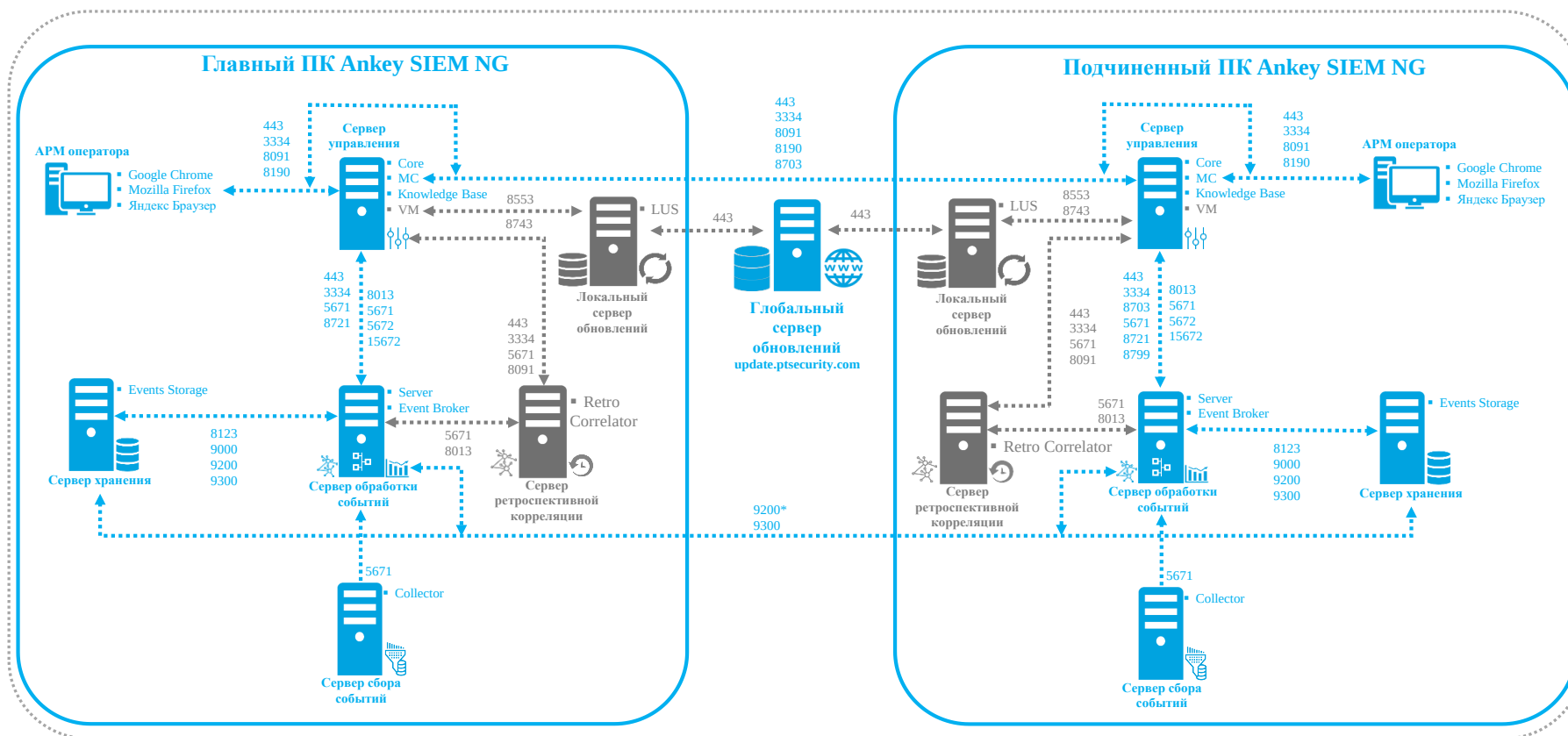


Рисунок 1.2 – Схема взаимодействия компонентов ПК Ankey SIEM NG в варианте исполнения Ankey SIEM NG с дополнительным компонентом VM

Взаимодействие компонентов двух ПК Ankey SIEM NG, расположенных на разных площадках и объединенных в одну иерархию, отражено на рисунке 2.1.



* Требуется для распределенного поиска событий в иерархии

Рисунок 2.1 – Схема взаимодействия компонентов двух ПК Ankey SIEM NG, которые объединены в одну иерархию⁴

⁴ компонент VM активен для исполнения Ankey SIEM NG с дополнительным компонентом VM и неактивен для исполнения Ankey SIEM NG.

Алгоритм взаимодействия:

1. Модули компонента Ankey SIEM NG Collector сканируют ИТ-инфраструктуру предприятия, собирают сведения о сетевых узлах и событиях с источников. Собранные данные коллекторы передают в Ankey SIEM NG Server и Ankey SIEM NG Core. Переданные события используются в Ankey SIEM NG Server для нормализации, агрегации, обогащения и корреляции.
2. Компонент Ankey SIEM NG Core обрабатывает и хранит результаты сканирования с подробной информацией об обнаруженных ОС, ПО, службах, портах и прочими сведениями об узлах и связях между ними. Также компонент хранит параметры задач на сбор данных, профилей сканирования и транспортов, данные и сценарии справочников и осуществляет контроль доступа к этим данным, связываясь с остальными компонентами системы для выполнения пользовательских запросов.
3. Компонент Ankey SIEM NG Server обрабатывает входящий поток событий, приводит их к единому формату в соответствии с правилами нормализации и группирует их согласно правилам агрегации. Он также связывает события с активами и, при необходимости, создает новые активы на основе событий. Затем дополняет данные о событиях, используя правила обогащения или табличные списки, и анализирует поток нормализованных событий по правилам корреляции для выявления и регистрации событий информационной безопасности. Ankey SIEM NG Server передает компоненту Ankey SIEM NG Events Storage поступившие события в исходном (необработанном) и в нормализованном виде для хранения.

Примечание. Нормализация событий может выполняться на сервере Ankey SIEM NG Collector. Для этого необходимо установить на сервер Ankey SIEM NG Collector облегченную версию Ankey SIEM NG Server – «SIEM на коллекторе». События, нормализованные на таком сервере Ankey SIEM NG Collector, передаются для агрегации, обогащения и корреляции на основной Ankey SIEM NG Server.

4. Компонент Knowledge Base содержит базу знаний, необходимых Ankey SIEM NG для структурирования сведений, собранных от источников событий и объектов инфраструктуры.
5. Компонент Ankey SIEM NG MC обеспечивает доступ к системе через сервис единого входа, журналирует действия пользователей, а в исполнении Ankey SIEM NG с дополнительным компонентом VM также хранит информацию об уязвимостях.
6. Для управления системой, просмотра данных, построения отчетов и мониторинга пользователь подключается к компоненту Ankey SIEM NG Core через веб-интерфейс в соответствии с правами, которые назначены в Ankey SIEM NG MC.

7. Компонент Ankey SIEM NG RC обеспечивает возможность ретроспективной проверки полученных ранее событий, используя новые правила корреляции и данные из табличных списков.

Для обеспечения сетевого взаимодействия компонентов ПК Ankey SIEM NG должны быть доступны для входящих соединений порты, которые представлены в таблице 1.2.

Таблица 1.2 – Компоненты и порты взаимодействия ПК Ankey SIEM NG

Источник	Получатель	TCP-порт
Рабочая станция пользователя, ПО для загрузки данных уведомлений	Ankey SIEM NG Core	443
Ankey SIEM NG Server	Ankey SIEM NG Core	443, 3334, 5671, 5672, 8721
Ankey SIEM NG RC	Ankey SIEM NG Core	443, 5671
Рабочая станция пользователя	Knowledge Base	8091, 8190
Ankey SIEM NG RC	Knowledge Base	8091
Рабочая станция пользователя, компонент Ankey SIEM NG RC	Ankey SIEM NG MC	3334
Ankey SIEM NG Core	Ankey SIEM NG Server	5671, 5672, 15672, 8013
Knowledge Base	Ankey SIEM NG Server	8013
Ankey SIEM NG RC	Ankey SIEM NG Server	8013, 5671
Ankey SIEM NG Collector	Ankey SIEM NG Server	5671
Ankey SIEM NG Server	Ankey SIEM NG Events Storage	8123, 9000, 9200, 9300
Ankey SIEM NG Core ⁵	Ankey SIEM NG Update Mirror (LUS)	8553, 8743
Ankey SIEM NG Update Mirror (LUS) ⁵	Глобальный сервер обновлений	443

Внимание! На сервере, на который необходимо установить роль Deployer, порты 4505/TCP, 4506/TCP, 5000/TCP должны быть доступны для входящих соединений.

Для взаимодействия между двумя площадками с ПК Ankey SIEM NG, которые

⁵ только в исполнении Ankey SIEM NG с дополнительным компонентом VM

объединены в одну иерархию, должны быть доступны для входящих соединений порты, которые представлены в таблице 1.3

Таблица 1.3 – Компоненты и порты для обеспечения взаимодействия между двумя ПК Ankey SIEM NG, объединенными в одну иерархию

Источник	Получатель	TCP-порт
Взаимодействие между двумя площадками с ПК Ankey SIEM NG, которые объединены в одну иерархию		
Ankey SIEM NG Core	Ankey SIEM NG Core	443, 3334, 8091, 8190, 8703
Ankey SIEM NG Events Storage	Ankey SIEM NG Events Storage	9200,9300

Для средненагруженных и высоконагруженных систем на серверах, на которые устанавливаются компоненты Ankey SIEM NG Server, Ankey SIEM NG Events Storage, Ankey SIEM NG Core, Ankey SIEM NG Collector, Ankey SIEM NG RC, порты 22/TCP, 4505/TCP, 4506/TCP должны быть открыты для входящих соединений.

Для исходящих соединений не требуется создавать правила межсетевого экрана. Для удаленного доступа к серверам компонентов рекомендуется разрешить соединения от рабочих станций администратора через порт 3389/TCP к серверам на Microsoft Windows, через порт 22/TCP – к серверам на Linux.

Для возможности репликации событий необходимо обеспечить сетевое взаимодействие через TCP-порты 5671 и 5672 между серверами Core связываемых приложений, а также между серверами Server связываемых приложений.

3 Развертывание ПК Ankey SIEM NG

В этом разделе приведены инструкции по установке компонентов ПК Ankey SIEM NG, активации лицензии и первоначальной настройке ключевых функций системы, даны рекомендации по выбору конфигурации, а также описаны типовые схемы развертывания, аппаратные и программные требования к серверам.

3.1 Типовые схемы развертывания ПК Ankey SIEM NG

В этом подразделе приведены рекомендации по выбору конфигурации ПК Ankey SIEM NG, описаны типовые схемы развертывания.

3.1.1 Рекомендации по выбору конфигурации ПК Ankey SIEM NG

В зависимости от сложности ИТ-инфраструктуры организации могут применяться 3 основные конфигурации ПК Ankey SIEM NG.

1) **Конфигурация для низконагруженных систем.**

Рекомендуется для развертывания в организациях, которые:

- планируют выполнять периодическое сканирование узлов не чаще одного раза в месяц и хранить в базе данных СУБД Jatoba или PostgreSQL не более 2000 активов;
- планируют получать общий поток событий от источников, не превышающий 5 000 событий в секунду⁶, и не планируют расширение своей ИТ-инфраструктуры.

Внимание! Если поток событий, который принимает ПК Ankey SIEM NG, превышает 70 % от допустимого потока для низконагруженной конфигурации, а также планируется установка или создание дополнительных правил корреляции помимо пакета общих ресурсов контента, то рекомендуется применять конфигурацию для средненагруженных или высоконагруженных систем (в зависимости от потока событий). Применение конфигурации для средненагруженных или высоконагруженных систем позволяет расширить возможности горизонтального или вертикального масштабирования SIEM-системы (включая новые функциональные возможности), а также увеличить общую пропускную способность и производительность.

⁶ не более 5 000 событий в секунду при использовании модуля syslog, не более 3 000 событий в секунду при смешанном сборе событий.

2) **Конфигурация для средненагруженных систем.**

Рекомендуется для развертывания в организациях, которые:

- планируют хранить в базе данных СУБД Jatoba или PostgreSQL не более 5 000 активов;
- планируют получать общий поток событий от источников, не превышающий 15 000 событий в секунду, и планируют расширение своей ИТ-инфраструктуры.

3) **Конфигурация для высоконагруженных систем.**

Рекомендуется для развертывания в организациях, которые:

- планируют хранить в базе данных СУБД Jatoba или PostgreSQL не более 20 000 активов⁷;
- планируют получать общий поток событий от источников, не превышающий 50 000 событий в секунду на один конвейер⁸, и планируют расширение своей ИТ-инфраструктуры.

3.1.2 Схема развертывания конфигурации для низконагруженных систем

Для развертывания конфигурации потребуется один сервер. На него необходимо установить основные компоненты:

- Ankey SIEM NG Core;
- Ankey SIEM NG Knowledge Base;
- Ankey SIEM NG MC;
- Ankey SIEM NG Server;
- Ankey SIEM NG Events Storage;
- Ankey SIEM NG Collector.

Для выполнения ретроспективной корреляции на отдельный сервер возможно установить дополнительный компонент Ankey SIEM NG RC. Установка этого компонента является необязательной.

Внимание! Компонент Ankey SIEM NG RC необходимо устанавливать на выделенный сервер, отдельно от серверов с компонентами Ankey SIEM NG Server и Ankey SIEM NG Collector.

Примечание. Количество серверов Ankey SIEM NG Collector зависит от планируемой нагрузки на коллекторы, а также от физической и логической топологии ИТ-инфраструктуры организации. Если требуется сканировать узлы, расположенные в отдельных сетевых сегментах, рекомендуется устанавливать отдельный коллектор на каждый сегмент. Максимально возможное количество коллекторов для одного экземпляра Ankey SIEM NG Core – 50.

Компоненты системы могут быть установлены в виртуальной среде (см. пункт 3.2.8).

⁷ В случае, если количество хранимых в Core активов превышает 20 000, необходимо увеличить объем вычислительных ресурсов (CPU, HDD, RAM), которые требуются для функционирования Core.

⁸ Если общий поток превышает 50 000 событий в секунду, рекомендуется развернуть дополнительные конвейеры обработки событий и распределить общий поток событий между всеми конвейерами (см. подраздел «Схема горизонтального масштабирования»).

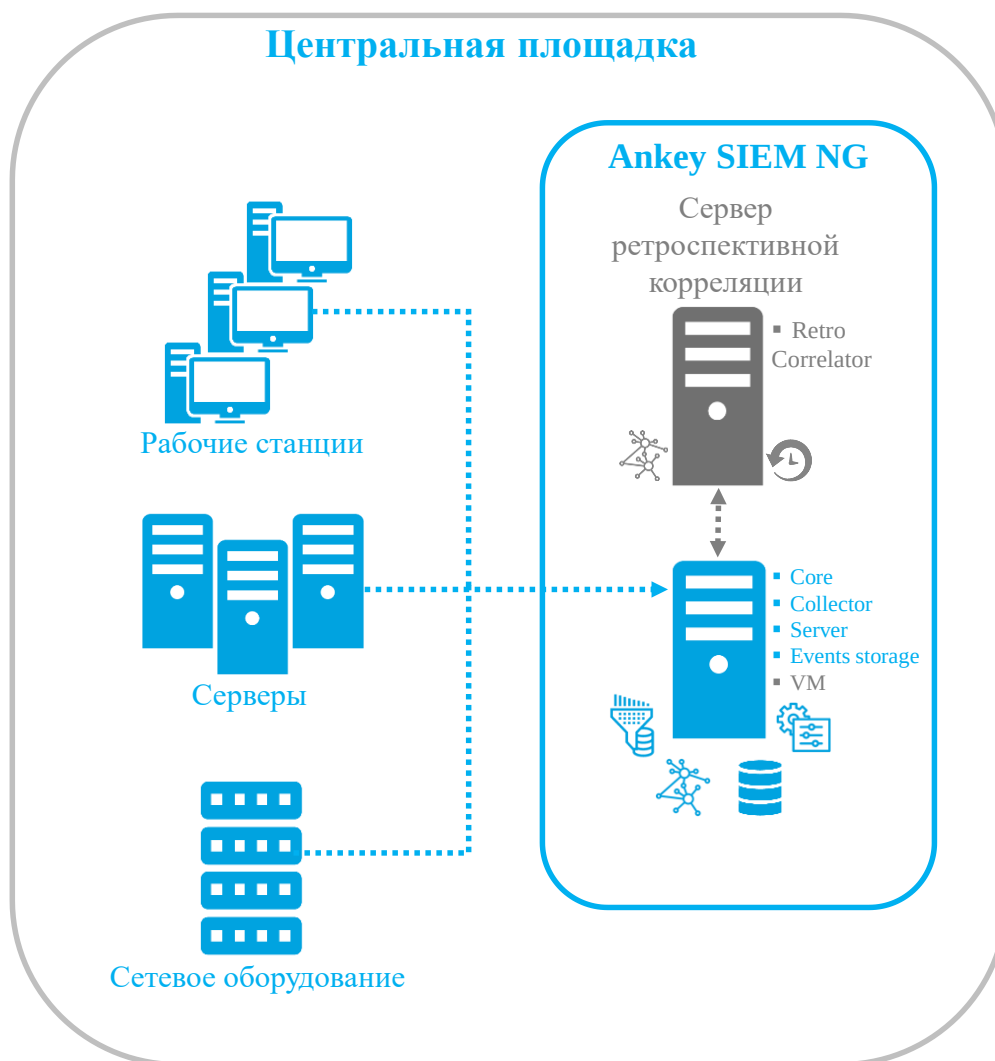


Рисунок 3.1 – Развертывание конфигурации для низконагруженных систем на одной площадке

Развертывание двух ПК Ankey SIEM NG, расположенных на разных площадках и объединенных в одну иерархию, отражено на рисунке 3.2.

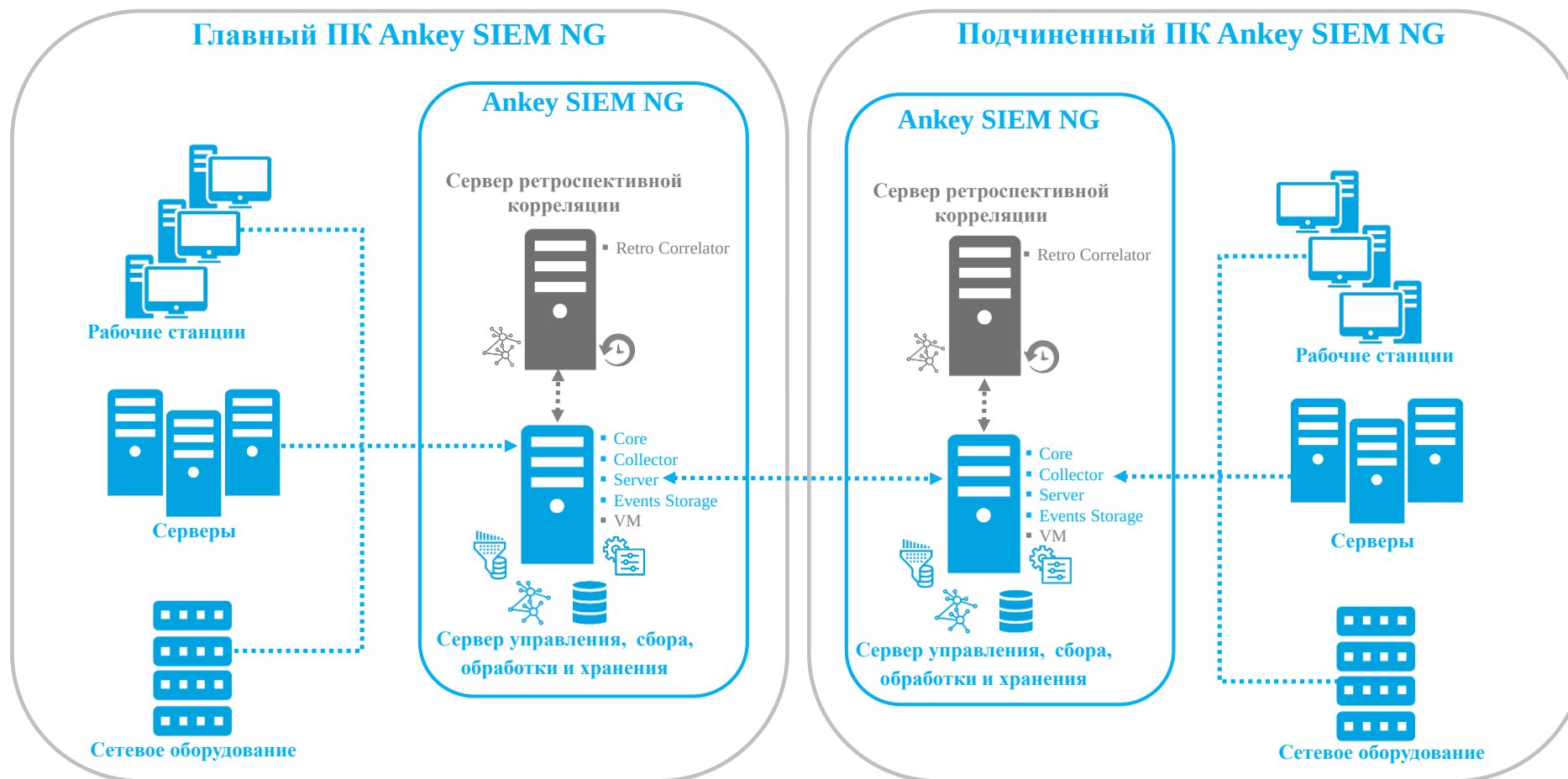


Рисунок 3.2 – Объединение двух ПК Ankey SIEM NG в конфигурации для низконагруженных систем в одну иерархию

В зависимости от физической или логической топологии ИТ-инфраструктуры организации может потребоваться сканировать узлы, расположенные в отдельных сетевых сегментах. В этом случае на каждый сегмент рекомендуется устанавливать отдельный коллектор⁹.

Количество серверов, требуемых для такой схемы развертывания, увеличивается на число дополнительных коллекторов.

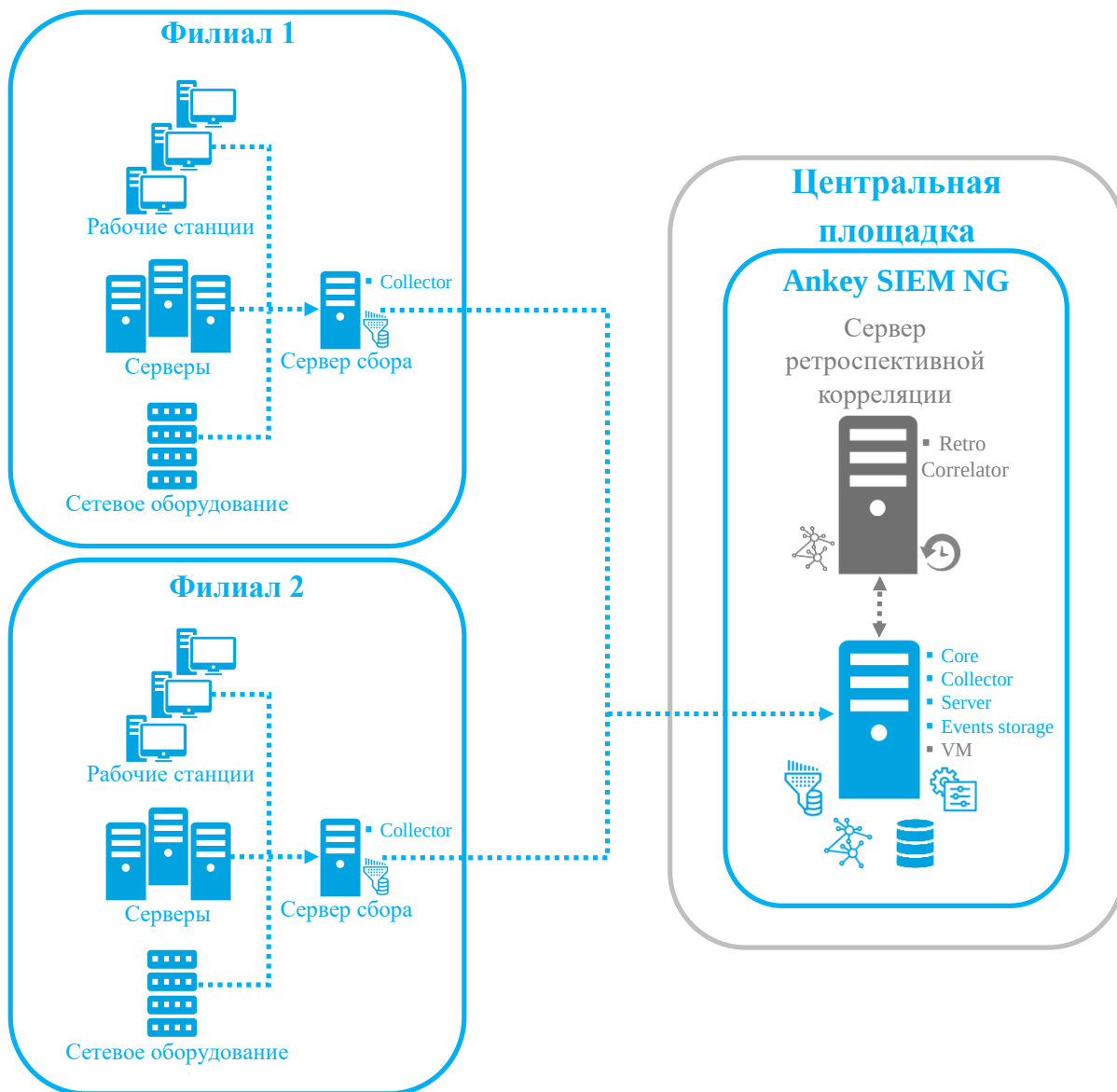


Рисунок 3.3 – Развертывание конфигурации для низконагруженных систем на филиальной сети

⁹ На одном коллекторе не рекомендуется одновременно запускать: более 4 задач с каждым модулем audit, pentest, customeventcollector, vshperevenetcollector; более 100 задач с модулями syslog, wineventlog, filemonitor, netflow, odbcblog, networkwatch, ssheventcollector, snmpcollector; более 1 задачи с каждым модулем hostdiscovery, batcheventsearch, dpicollector, mp8scanimporter. ввиду потребления большого количества оперативной памяти, что требуется учитывать при выборе архитектуры программного комплекса с учетом распределения компонентов в инфраструктуре.

3.1.3 Схема развертывания конфигурации для средненагруженных систем

Для развертывания ПК Ankey SIEM NG в средненагруженной конфигурации потребуются минимум три сервера.

На первый сервер необходимо установить основные компоненты:

- Ankey SIEM NG Core;
- Knowledge Base;
- Ankey SIEM NG MC;
- Ankey SIEM NG Collector;

на второй – основные компоненты

- Ankey SIEM NG Server;
- Ankey SIEM NG Events Storage;

на третий – дополнительный компонент

- Ankey SIEM NG Collector.

Количество дополнительных компонентов Ankey SIEM NG Collector будет зависеть от общего потока событий на весь ПК Ankey SIEM NG. При общем потоке 10 000 событий в секунду всего потребуется четыре компонента Ankey SIEM NG Collector с распределением потока между ними (не более 2 500 событий в секунду на один Ankey SIEM NG Collector).

Для выполнения ретроспективной корреляции на отдельный сервер возможно установить дополнительный компонент Ankey SIEM NG RC. Установка этого компонента необязательна.

Внимание! Компонент Ankey SIEM NG RC необходимо устанавливать на выделенный сервер, отдельно от серверов с компонентами Ankey SIEM NG Server и Ankey SIEM NG Collector.

Примечание. Количество серверов Ankey SIEM NG Collector зависит от планируемой нагрузки на коллекторы, а также от физической и логической топологии ИТ-инфраструктуры организации. Если требуется сканировать узлы, расположенные в отдельных сетевых сегментах, рекомендуется устанавливать отдельный коллектор на каждый сегмент. Максимально возможное количество коллекторов для одного экземпляра Ankey SIEM NG Core – 50.

Компоненты системы могут быть установлены в виртуальной среде (см. пункт 3.2.8).

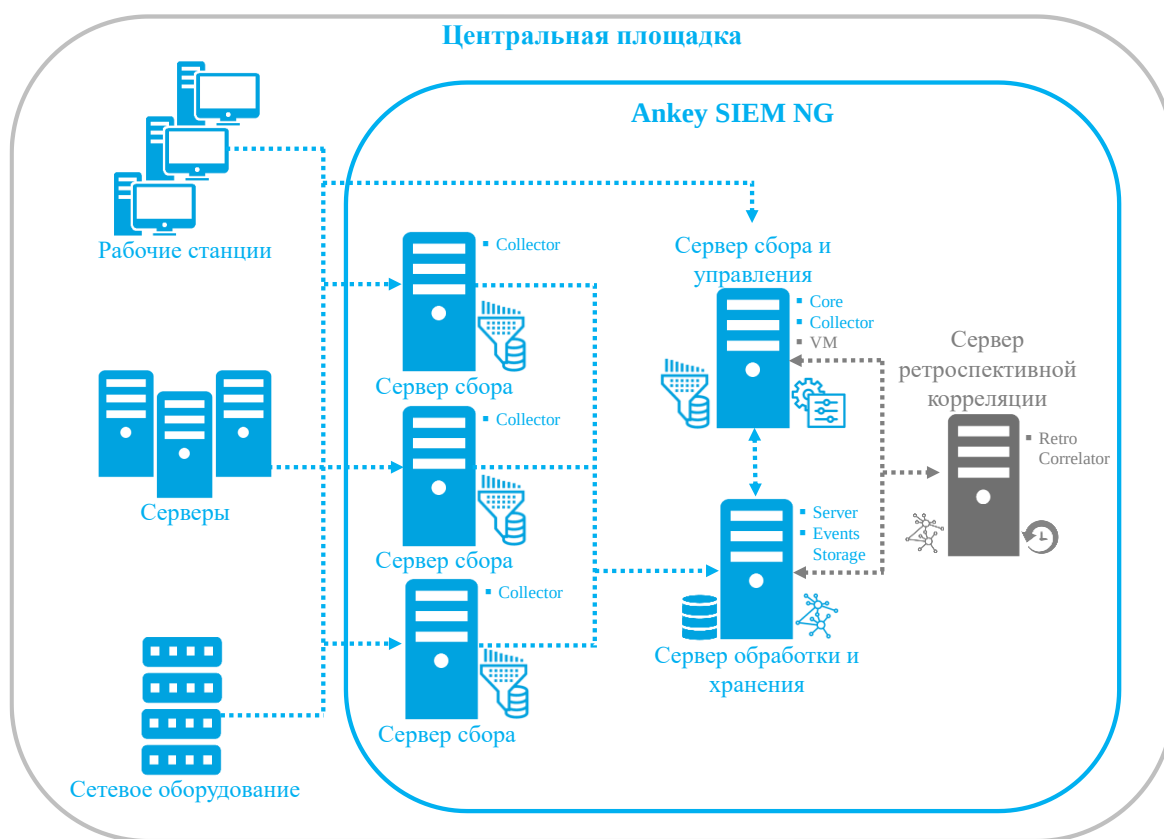


Рисунок 3.4 – Развертывание конфигурации для средненагруженных систем на одной площадке

Развертывание двух ПК Ankey SIEM NG, расположенных на разных площадках и объединенных в одну иерархию, отражено на рисунке 3.5.

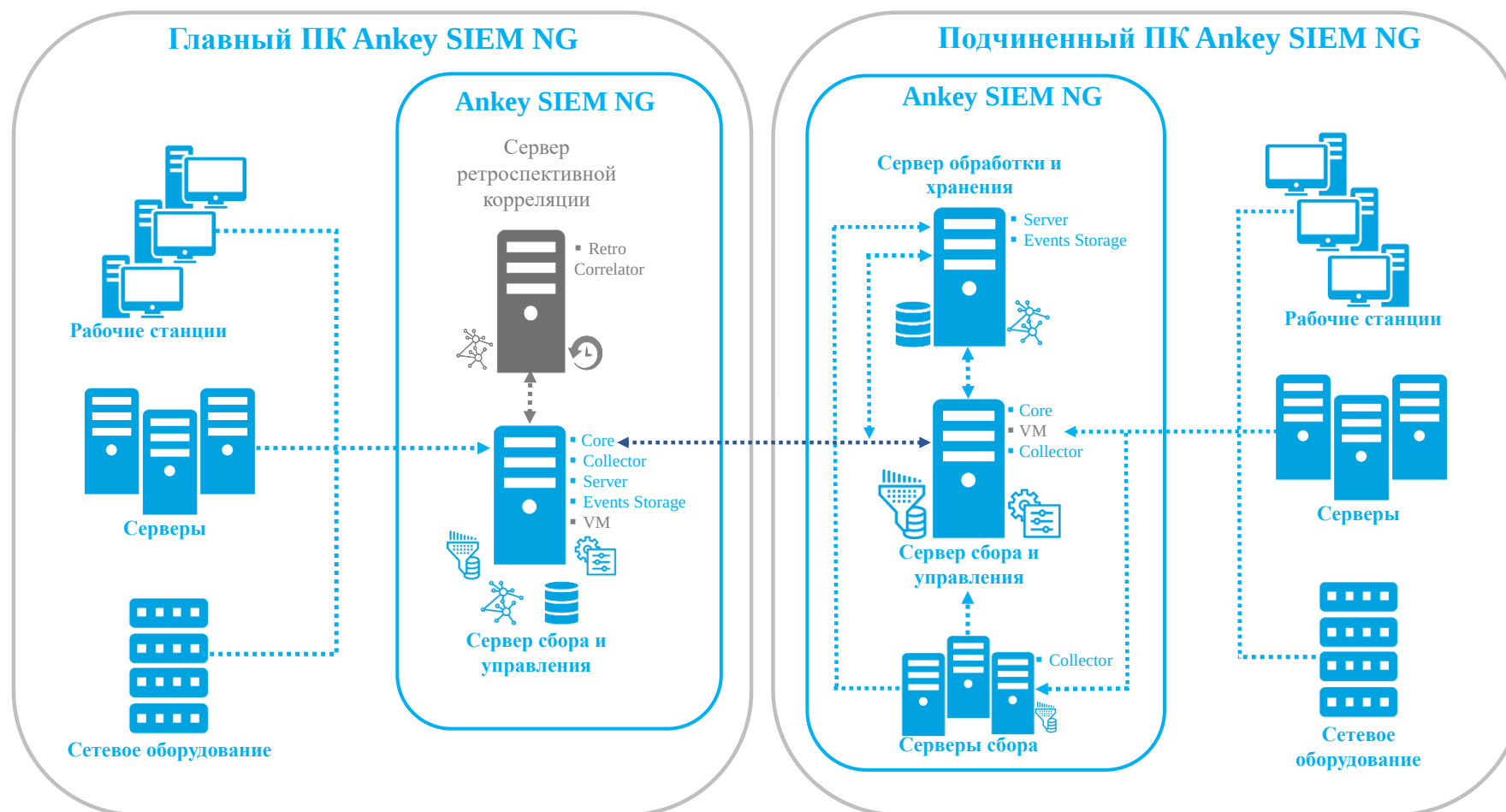


Рисунок 3.5 – Объединение ПК Ankey SIEM NG в конфигурации для низконагруженных и ПК Ankey SIEM NG в конфигурации для средненагруженных систем в одну иерархию.

В зависимости от физической или логической топологии ИТ-инфраструктуры организации может потребоваться сканировать узлы, расположенные в отдельных сетевых сегментах. В этом случае на каждый сегмент рекомендуется устанавливать отдельный коллектор¹⁰.

Количество серверов, требуемых для такой схемы развертывания, увеличивается на число дополнительных коллекторов.

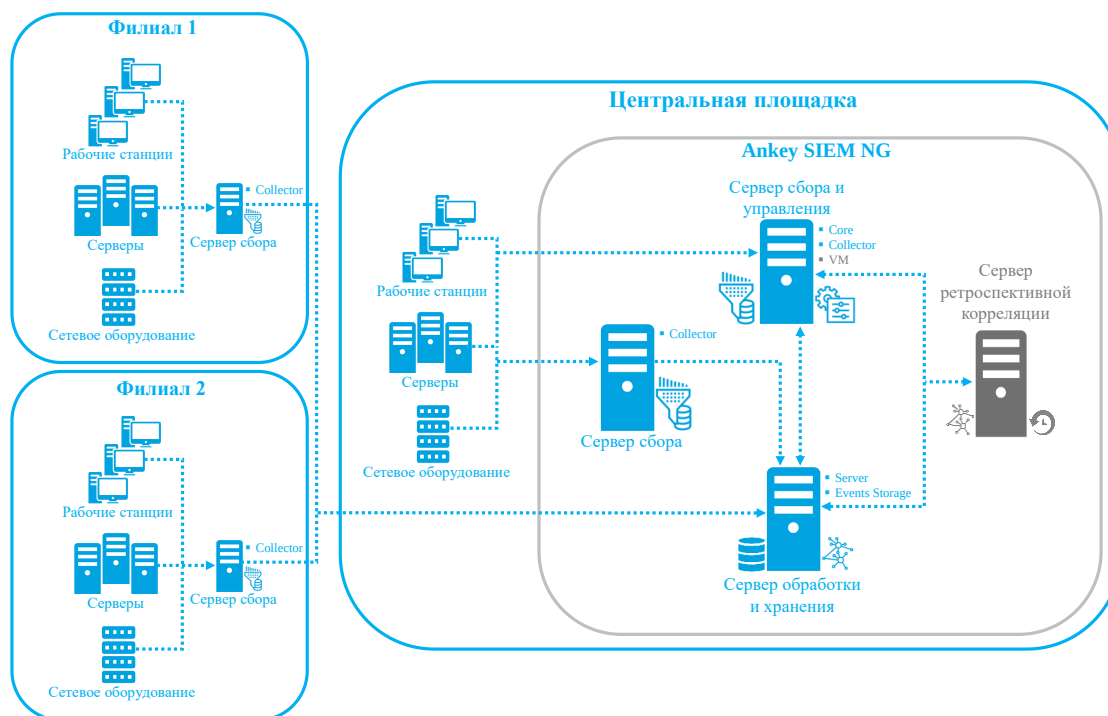


Рисунок 3.6 – Развертывание конфигурации для средненагруженных систем на филиальной сети

¹⁰ На одном коллекторе не рекомендуется одновременно запускать: более 4 задач с каждым модулем audit, pentest, customeventcollector, vshperevenetcollector; более 100 задач с модулями syslog, wineventlog, filemonitor, netflow, odbclg, networkwatch, ssheventcollector, snmpeventcollector; более 1 задачи с каждым модулем hostdiscovery, batcheventsearch, dpicollector, mp8scanimporter. ввиду потребления большого количества оперативной памяти, что требуется учитывать при выборе архитектуры программного комплекса с учетом распределения компонентов в инфраструктуре.

3.1.4 Схема развертывания конфигураций для высоконагруженных систем

Для развертывания конфигураций вам потребуются:

- сервер для компонентов Ankey SIEM NG Core, Ankey SIEM NG Knowledge Base и Ankey SIEM NG MC;
- сервер для компонента Ankey SIEM NG Server;
- сервер для компонента Ankey SIEM NG Events Storage;
- серверы для компонентов Ankey SIEM NG Collector.

Примечание. Количество серверов Ankey SIEM NG Collector зависит от планируемой нагрузки на коллекторы, а также от физической и логической топологии ИТ-инфраструктуры организации. Если требуется сканировать узлы, расположенные в отдельных сетевых сегментах, рекомендуется устанавливать отдельный коллектор на каждый сегмент. Максимально возможное количество коллекторов для одного экземпляра Ankey SIEM NG Core – 50.

Количество серверов для компонентов Ankey SIEM NG Collector¹¹ зависит от планируемой нагрузки на коллекторы, а также от физической и логической топологии ИТ-инфраструктуры организации. В конфигурации для высоконагруженных систем при общем потоке до 50 000 событий в секунду потребуется распределить весь поток событий между 20 серверами с компонентом Ankey SIEM NG Collector (не более 2 500 событий в секунду на 1 Ankey SIEM NG Collector).

Если требуется сканировать узлы, расположенные в отдельных сетевых сегментах, рекомендуется устанавливать отдельный коллектор на каждый сегмент.

Для выполнения ретроспективной корреляции на отдельный сервер возможно установить дополнительный компонент Ankey SIEM NG RC. Установка этого компонента необязательна.

Внимание! Компонент Ankey SIEM NG RC необходимо устанавливать на выделенный сервер, отдельно от серверов с компонентами Ankey SIEM NG Server и Ankey SIEM NG Collector.

¹¹ На одном коллекторе не рекомендуется одновременно запускать: более 4 задач с каждым модулем audit, pentest, customeventcollector, vshperevenetcollector; более 100 задач с модулями syslog, wineventlog, filemonitor, netflow, odcblog, networkwatch, ssheventcollector, snmpeventcollector; более 1 задачи с каждым модулем hostdiscovery, batcheventsearch, dpicollector, mp8scanimporter. ввиду потребления большого количества оперативной памяти, что требуется учитывать при выборе архитектуры программного комплекса с учетом распределения компонентов в инфраструктуре.

Компоненты системы могут быть установлены в виртуальной среде (см. пункт 3.2.8).

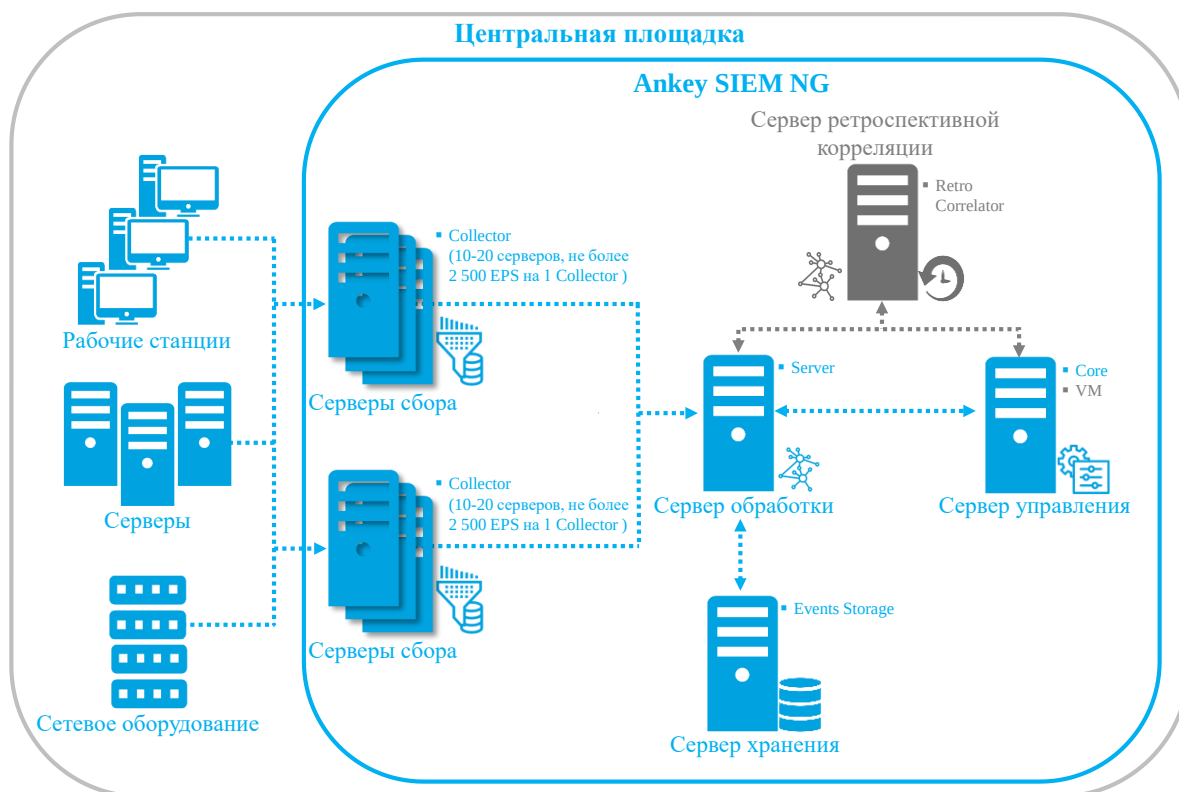


Рисунок 3.7 – Развертывание конфигурации для высоконагруженных систем (не более 2 500 событий в секунду на 1 Ankey SIEM NG Collector)

Развертывание двух ПК Ankey SIEM NG, расположенных на разных площадках и объединенных в одну иерархию, отражено на рисунках 3.8, 3.9.

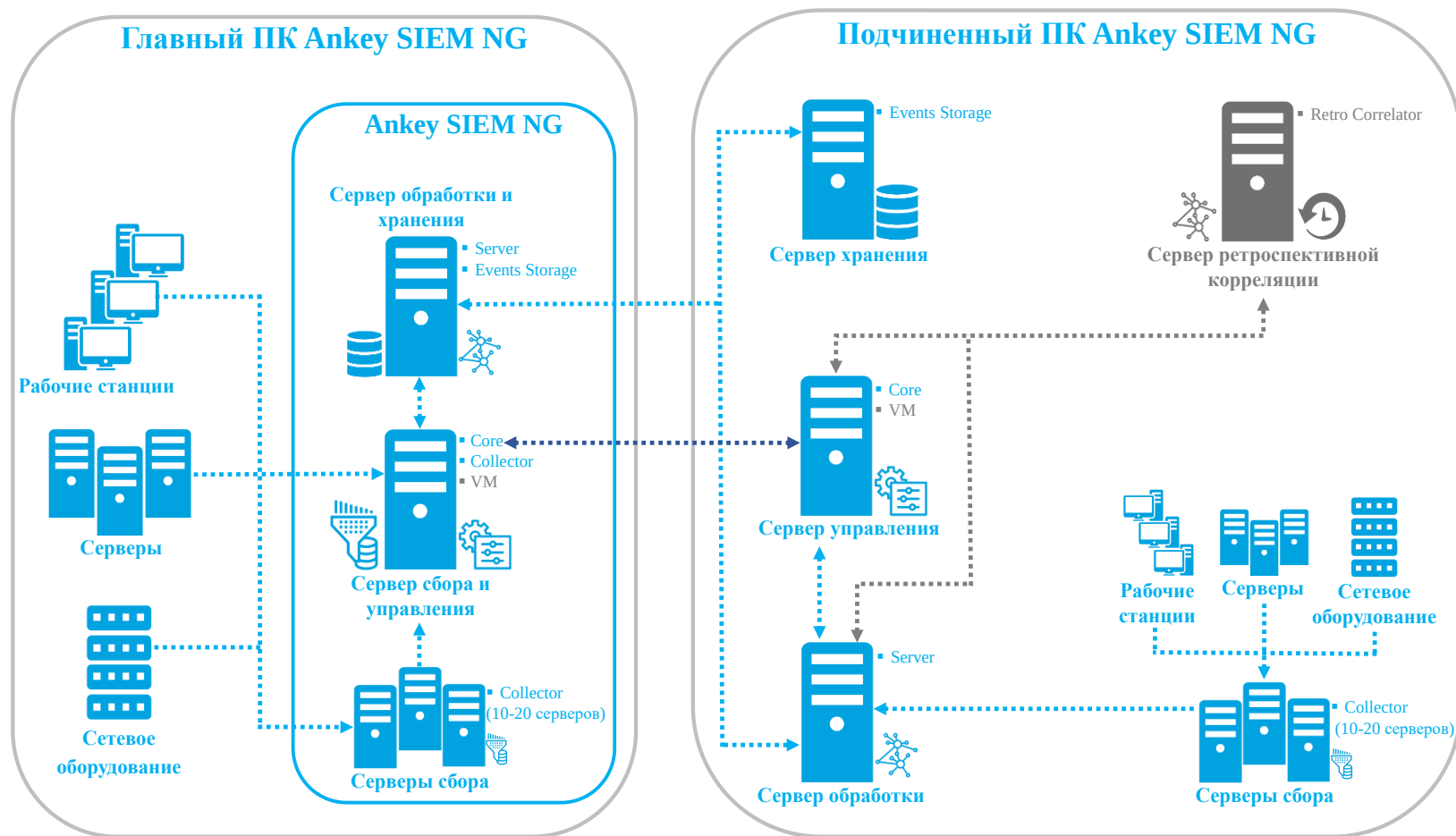


Рисунок 3.8 – Объединение ПК Ankey SIEM NG в конфигурации для средненагруженных систем и ПК Ankey SIEM NG в конфигурации для высоконагруженных систем в одну иерархию

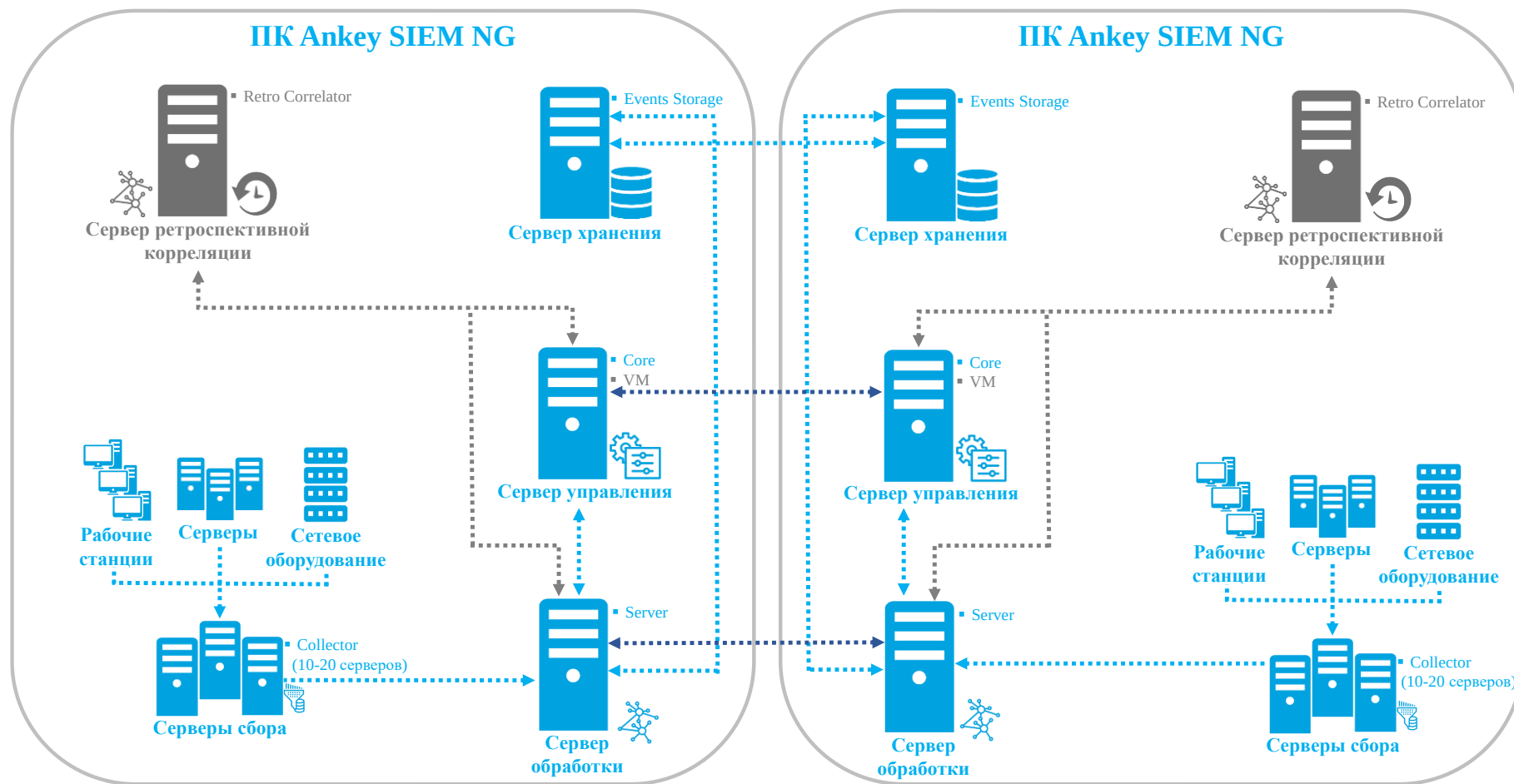


Рисунок 3.9 – Объединение двух ПК Ankey SIEM NG в конфигурации для средненагруженных в одну иерархию

3.1.5 Схемы масштабирования Ankey SIEM NG

Для крупных организаций может потребоваться более сложная схема развертывания, чтобы обеспечить эффективное управление интенсивным потоком событий и возможность гибкой настройки иерархии.

Крупным организациям может не хватить обычной схемы развертывания для управления большим потоком событий и гибкой настройки иерархии.

В случае необходимости в обработке крупного потока событий (свыше 50.000 событий в секунду), сбора и хранения событий на территориально удаленном филиале или для обеспечения возможности гибкой настройки иерархии, в Ankey SIEM NG есть возможность применить следующие схемы масштабирования Системы:

1. **Схема горизонтального масштабирования**
(см. подраздел 3.1.5.1)

Если общий поток событий от источников превышает 50.000 событий в секунду, его рекомендуется распределить между конвейерами обработки событий.

Также горизонтальное масштабирование возможно применить для организации на каждом территориально удаленном филиале сбора, обработки и хранения событий, сгенерированных на активах этого филиала

Развертывание системы горизонтально на нескольких конвейерах позволяет равномерно распределить нагрузку между ними и в то же время использовать единый сервер для хранения сведений обо всех активах и инцидентах, для управления задачами сканирования ИТ-инфраструктуры и сбора событий, а также для просмотра и анализа событий.

2. **Схема вертикального масштабирования**
(см. подраздел 3.1.5.2)

Если в крупной организации есть необходимость в централизованном контроле территориально удаленных филиалов и создании связей между ними, рекомендуется развернуть в каждом подразделении локальную площадку Ankey SIEM NG и объединить локальные площадки в иерархию.

3.1.5.1 Схема горизонтального масштабирования

Схема горизонтального масштабирования SIEM-системы (далее также – «горизонтальный SIEM») включает в себя один сервер управления Ankey SIEM NG Core и необходимое для ИТ-инфраструктуры количество конвейеров обработки событий (подробнее см. подраздел «**О конвейерах обработки событий**»).

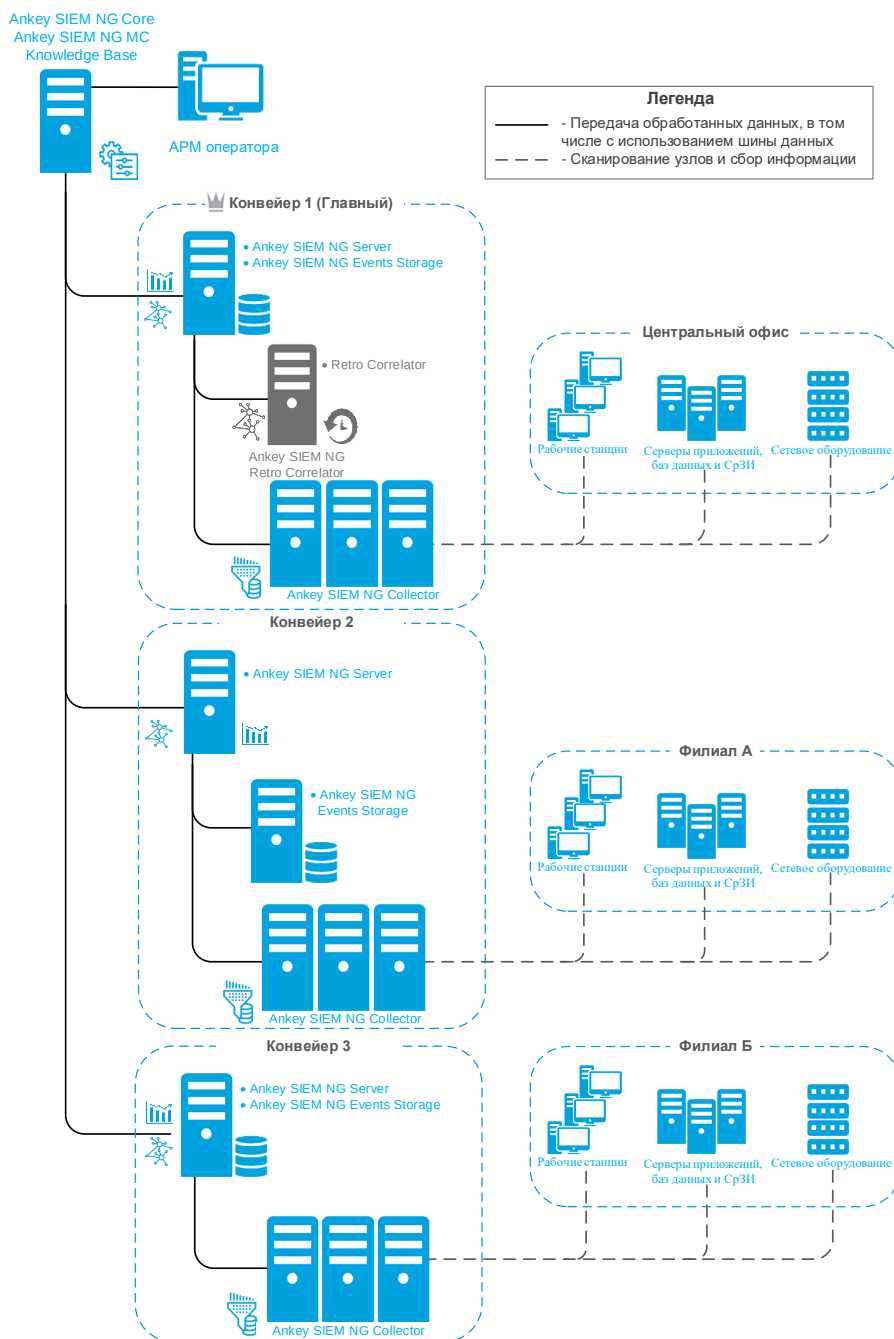


Рисунок 1.3 – Пример схемы масштабирования «Горизонтальный SIEM», развернутой с тремя конвейерами обработки событий

О конвейерах обработки событий

Конвейер обработки событий представляет собой совокупность компонентов Ankey SIEM NG Events Storage и Ankey SIEM NG Server с подключенными к нему компонентами Ankey SIEM NG Collector. Возможно также дополнительно установить в конвейер компонент Ankey SIEM NG Retro Correlator.

По умолчанию в состав ПК Ankey SIEM NG входит только один конвейер обработки событий. В конфигурациях для средненагруженных и высоконагруженных систем вы можете масштабировать Систему, установив один или несколько дополнительных конвейеров.

Внимание! Максимальный поток событий на один конвейер не должен превышать 50.000 событий в секунду.

Конвейер можно установить в каждом территориально удаленном филиале организации для сбора, обработки и хранения событий, сгенерированных на активах этого филиала. Работой всех конвейеров управляет единый управляющий сервер с компонентом Ankey SIEM NG Core, установленный в центральном офисе. Кроме того, каждый конвейер отправляет на управляющий сервер сведения об активах своего филиала. В центральном офисе также может быть установлен свой конвейер для обработки событий, произошедших в ИТ-инфраструктуре этого офиса.

Вы можете добавить один или несколько конвейеров в существующую систему (например, в случае расширения ИТ-инфраструктуры) или изначально развернуть систему с несколькими конвейерами обработки событий. Количество дополнительных конвейеров обработки событий ограничено лицензиями.

Один из конвейеров является главным, поскольку через компонент Ankey SIEM NG ES этого конвейера выполняются все запросы по фильтрации событий, в том числе хранящихся в других конвейерах (кросс-кластерный поиск). По умолчанию главным является первый установленный конвейер.

Рекомендации к установке конвейеров событий

Внимание! Не рекомендуется устанавливать дополнительные конвейеры в конфигурации для низконагруженных систем (такая схема развертывания не поддерживается производителем).

Внимание! Аппаратное обеспечение серверов каждого конвейера должно соответствовать потоку собираемых и обрабатываемых им событий.

Компоненты конвейера необходимо устанавливать в следующем порядке:

1. Ankey SIEM NG Events Storage;
2. Ankey SIEM NG Server;
3. Ankey SIEM NG Collector;
4. Ankey SIEM NG RC. Установка этого компонента необязательна.

Внимание! Компонент Ankey SIEM NG RC необходимо устанавливать на выделенный сервер, отдельно от серверов с компонентами Ankey SIEM NG Server и Ankey SIEM NG Collector.

Компоненты Ankey SIEM NG Server и Ankey SIEM NG ES могут быть установлены как на один сервер (в конфигурации для средненагруженных систем), так и на отдельные серверы (в конфигурации для высоконагруженных систем). Коллекторы рекомендуется устанавливать на отдельные серверы¹².

Если в Ankey SIEM NG установлены дополнительные конвейеры, между конвейерами должны быть доступны для входящих соединений порты 9200, 9300, 9320, 9340, 9341. Если кластер Elasticsearch сервера Ankey SIEM NG ES содержит четыре узла данных, также должны быть доступны порты 9342 и 9343.

¹² Установка коллектора на один сервер с компонентами Ankey SIEM NG Server, Ankey SIEM NG ES и Event Broker не рекомендуется, так как такая установка не предусмотрена архитектурно, что может привести к затруднению в работе модуля Salt при установке, а также Event Broker при эксплуатации.

3.1.5.2 Схема вертикального масштабирования

Схема вертикального масштабирования SIEM-системы (далее также – «вертикальный SIEM») включает в себя центральный сервер управления Ankey SIEM NG Core, который взаимодействует с серверами Ankey SIEM NG Core на подчиненных площадках. Каждая подчиненная площадка является полноценной установкой ПК Ankey SIEM NG, имеет свой управляющий сервер Ankey SIEM NG Core и свою базу активов и инцидентов. Площадки связываются между собой с помощью компонентов Ankey SIEM NG MC.

Для каждой площадки, включенной в схему «вертикальный SIEM», возможно развернуть один конвейер по умолчанию или применить схему горизонтального масштабирования внутри площадки.

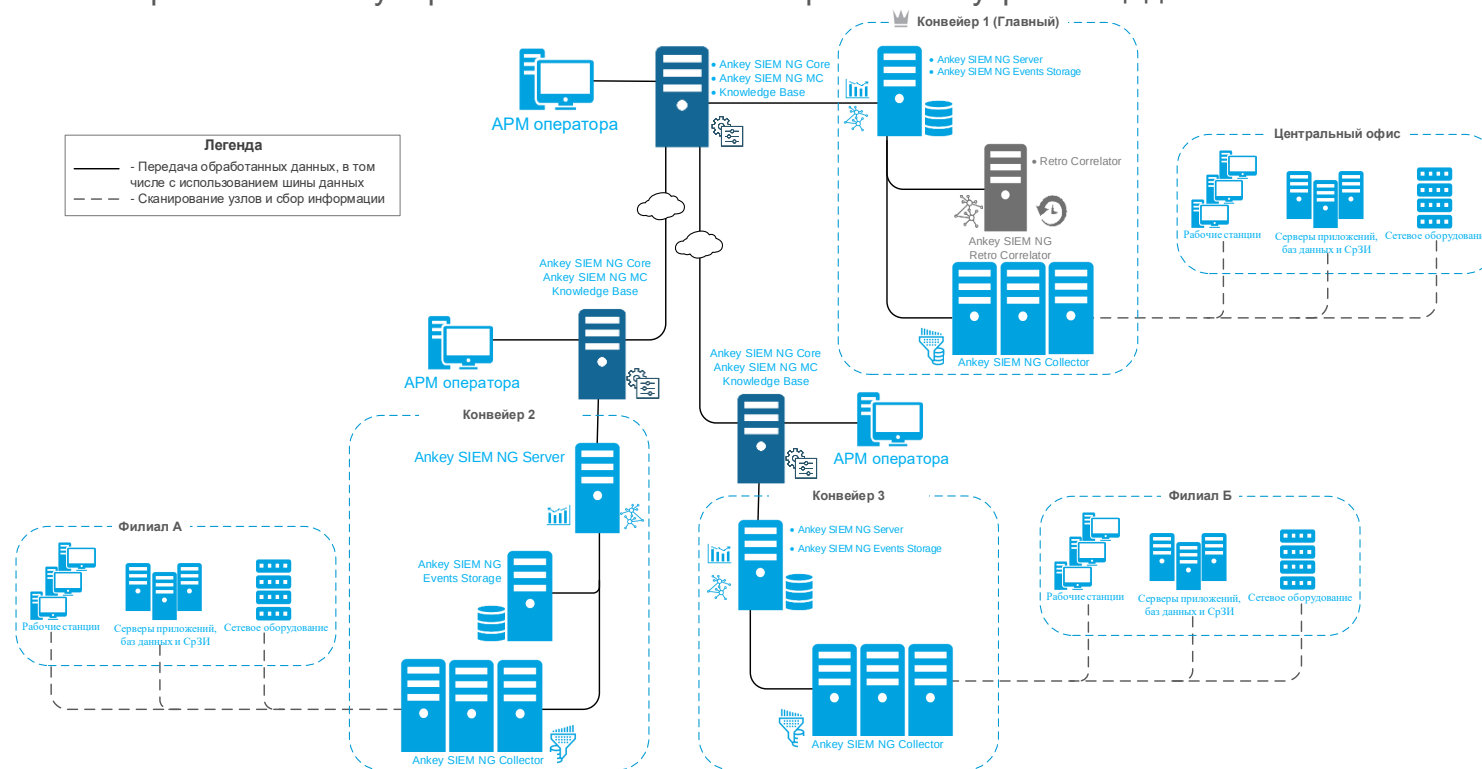


Рисунок 1.4 – Пример схемы «Вертикальный SIEM», развернутой с тремя конвейерами обработки событий

3.2 Аппаратные и программные требования

В этом подразделе приведены минимальные требования к аппаратному и программному обеспечению ПК Ankey SIEM NG. Не допускается применять вычислительные ресурсы ниже минимальных. В условиях активной эксплуатации ПК Ankey SIEM NG (в том числе несколькими пользователями одновременно) и при наличии частых пиковых нагрузок рекомендуется увеличить объем вычислительных ресурсов или изменить конфигурацию ПК Ankey SIEM NG на более производительную (например, с низконагруженной до средненагруженной). Итоговое решение об увеличении требований к минимальным вычислительным ресурсам для аппаратных платформ принимается эксплуатирующей организацией, которая будет эксплуатировать ПК Ankey SIEM NG или интегратором, на основе анализа проекта с учетом его особенностей, потребностей в установке дополнительных сервисов и включения расширенных функций ПК Ankey SIEM NG.

3.2.1 Требования к программному обеспечению и среде установки

Все компоненты Ankey SIEM NG поддерживают установку на 64-разрядные ОС семейства Linux – Astra Linux Special Edition 1.7.5 (на базе ядра Linux версии 5.15) или Debian 10.3–10.13 (на базе ядра Linux версии 5.10). Кроме того, вы можете установить компонент Ankey SIEM NG Collector и облегченную версию Ankey SIEM NG Server («SIEM на коллекторе») на Microsoft Windows Server 2012, 2012 R2, 2016, 2019 или 2022.

Для работы в интерфейсе ПК Ankey SIEM NG рекомендуется использовать последние версии браузеров Google Chrome, Mozilla Firefox, Microsoft Chromium Edge или Яндекс.Браузер.

3.2.1.1 Рекомендации к установке ПК Ankey SIEM NG на ОС Astra Linux SE

Установку и администрирование ОС Astra Linux SE версий необходимо осуществлять согласно официальной документации производителя¹³.

Перед развертыванием ПК Ankey SIEM NG на Astra Linux Special Edition 1.7 необходимо на серверах компонентов выполнить действия, указанные в актуальных бюллетенях производителя (последний актуальный бюллетень [№ 2024-0212SE17MD](#), подробнее см. [в справочном центре Astra Linux](#)).

¹³ Официальная документация для Astra Linux SE версий 1.7.x представлена в [справочном центре Astra Linux](#).

Рекомендации к установке базовой системы и выбору ядра

При установке ОС Astra Linux необходимо выбрать тип ядра **generic**. Тип ядра **hardened** не поддерживается ПК Ankey SIEM NG.

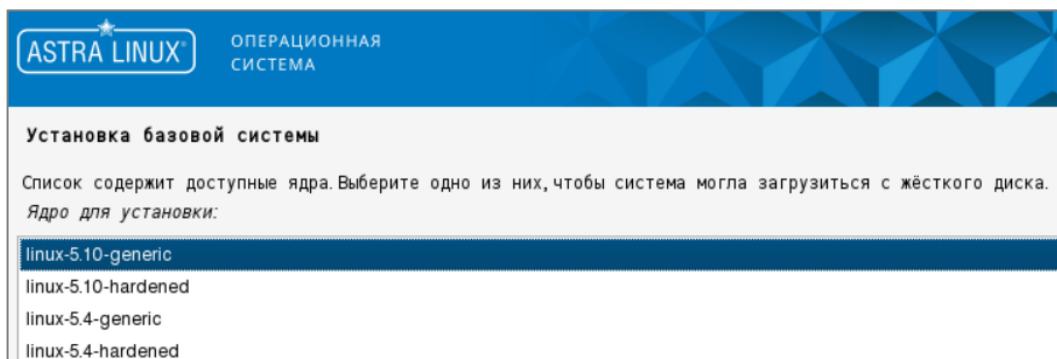


Рисунок 3.10 – Выбор типа ядра при установке ОС

Рекомендации к выбору дополнительных настроек ОС

Уровень защищенности ОС влияет на перечень дополнительных настроек, доступных для выбора. Рекомендуется использовать максимальный уровень защищенности «Смоленск» для более гибкой настройки ОС.

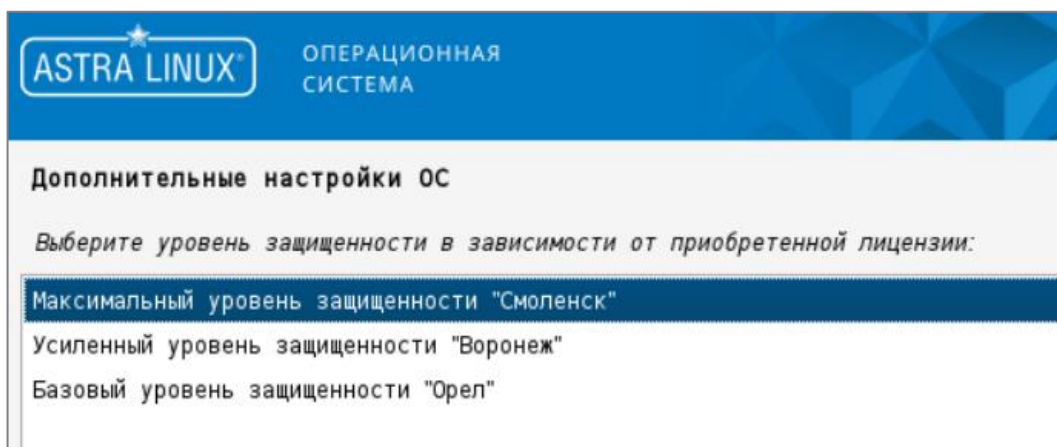


Рисунок 3.11 –Выбор уровня защищенности

Вы можете настроить параметры безопасности ОС с учетом особенностей проекта или сохранить настройки, заданные по умолчанию для выбранного уровня безопасности.

Внимание! Параметр **Запрос пароля для команды sudo** должен быть отключен, как показано на рисунке 3.12.

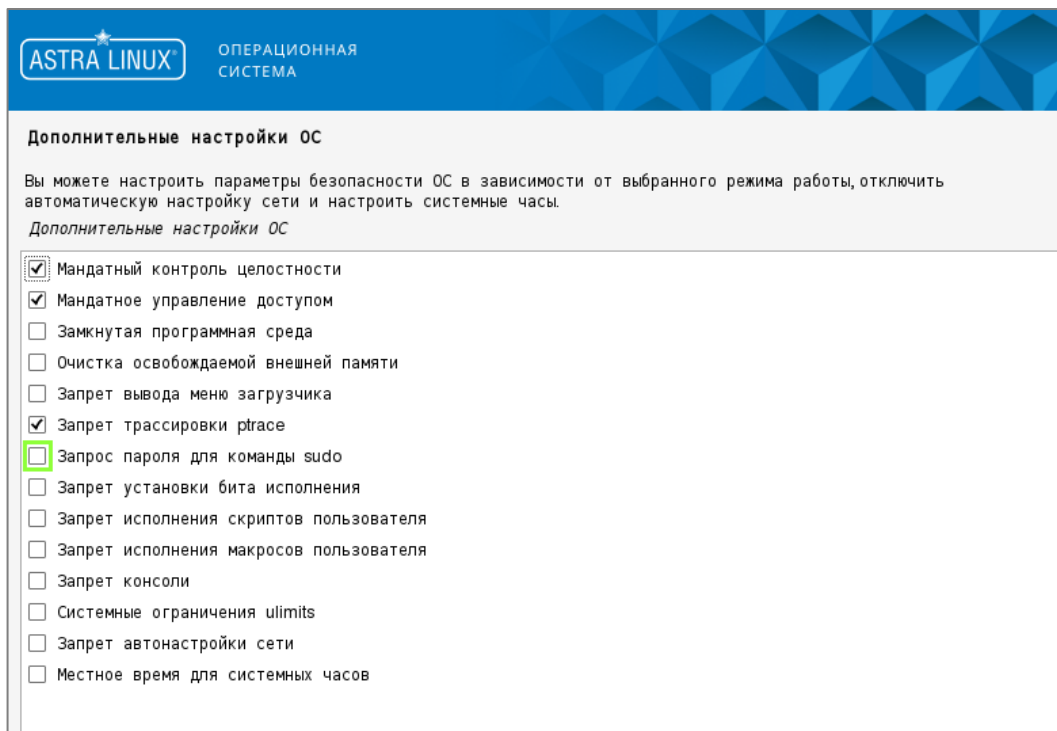


Рисунок 3.12 – Дополнительные настройки ОС Astra Linux

Если операционная система Astra Linux была установлена с активированным параметром **Запрос пароля для команды sudo**, то его можно отключить с помощью команды `sudo astra-sudo-control disable` в интерфейсе командной строки операционной системы.

После установки всех компонентов ПК, в случае необходимости, запрос пароля для команды `sudo` возможно включить в уже установленной операционной системе с помощью команды `sudo astra-sudo-control enable`, которую следует выполнить в интерфейсе командной строки с правами суперпользователя.

Если при установке ОС Astra Linux был включен параметр **Мандатный контроль целостности**, то для учетной записи, которая используется при установке компонентов системы, необходимо выбрать максимальный уровень целостности.

Рекомендации к настройке репозиториев

Перед началом установки ролей ПК необходимо корректно настроить репозитории для ОС Linux. Полная информация о настройке репозиториев Astra Linux приведена [в справочном центре Astra Linux](#).

В случае наличия доступа к глобальной сети Интернет в файле `sources.list` следует проверить наличие или добавить адреса [Интернет-репозиториев для ОС Astra Linux SE](#):

```
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-main/ 1.7_x86-64
main contrib non-free
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-update/ 1.7_x86-64
main contrib non-free
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-base/ 1.7_x86-64
main contrib non-free
```

deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-extended/ 1.7_x86-64 main contrib non-free

Все остальные ссылки следует закомментировать или удалить.

На время процесса установки ПК Ankey SIEM NG рекомендуется отключить обновление ОС Astra Linux SE из интернет-репозитория.

В случае отсутствия доступа к глобальной сети Интернет необходимо настроить локальный репозиторий ОС Astra Linux SE. Для этого необходимо создать каталог и распаковать в него архив с пакетами локального репозитория. Далее в файл `/etc/apt/sources.list` следует добавить ссылку на каталог, в котором содержатся пакеты локального репозитория. Например, `deb [trusted=yes] file:<Полный путь до каталога с локальным репозиторием> main non-free`.

Все остальные ссылки следует закомментировать или удалить.

3.2.1.2 Рекомендации к установке ПК на ОС Debian

Для установки или обновления Debian необходимо использовать полный установочный образ. Он содержит необходимый набор пакетов и не требует подключения к интернету (подробнее см. на сайте debian.org).

Если в Debian 10.3–10.13 используется версия ядра ниже требуемой, перед установкой или обновлением Ankey SIEM NG необходимо обновить его версию, установив метапакет ядра `linux-image-5.10-amd64`. При обновлении версии ядра не требуется обновление ОС.

3.2.2 Требования к аппаратному обеспечению конфигурации для низконагруженных систем

Компоненты системы необходимо устанавливать на серверы или в виртуальную среду, которые удовлетворяют приведенным ниже аппаратным требованиям.

Внимание! Установка компонентов системы возможна только на серверы с процессорами, поддерживающими инструкции SSE 4.2.

Core, MC, KB, Server, ES, Collector (до 5000 EPS, до 2000 активов). Требования

Таблица 3.1 – Аппаратные требования к серверу сбора, управления, обработки и хранения событий с компонентами Ankey SIEM NG Core, Ankey SIEM NG MC, Ankey SIEM NG Knowledge Base, Ankey SIEM NG Server, Ankey SIEM NG Events Storage и Ankey SIEM NG Collector при общем потоке **до 5 000 событий в секунду** и общем количестве активов в СУБД Jatoba или PostgreSQL **до 2 000 единиц**.

	Минимальные требования	
	До 2 000 событий в секунду (до 1000 активов)	До 5 000 событий в секунду (до 2000 активов)
Центральные процессоры	В процессоре(ах) должна быть реализована поддержка инструкций SSE4.2 и AVX и технология многопоточности, тактовая частота не менее 2,2 ГГц.	
Количество логических ядер в системе виртуализации	24	32
Память (ОЗУ)	64	96
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый	
Твердотельный накопитель для ОС и установки ПО	не менее 800 ГБ¹	
Жесткий диск для хранения событий (Elasticsearch)	<u>Расчетные значения³:</u> 250 EPS – в оперативном доступе: не менее 725 ГБ; – в архивах ⁴ : не менее 2 175 ГБ.	<u>Расчетные значения³:</u> 2 500 EPS – в оперативном доступе: не менее 7 242 ГБ; – в архивах ⁴ : не менее 21 726 ГБ.
Примечание. Чтобы определить требуемый объем свободного дискового пространства для хранения событий в оперативном доступе ² и выбрать накопителя для хранения событий (в		

компоненте Events Storage) следуйте инструкциям в пункте 3.2.7	1 000 EPS – <i>в оперативном доступе</i>: не менее 2 897 ГБ; – <i>в архивах</i>⁴: не менее 8 869 ГБ. 2 000 EPS – <i>в оперативном доступе</i>: не менее 5 794 ГБ; – <i>в архивах</i>⁴: не менее 17 382 ГБ	3 500 EPS – <i>в оперативном доступе</i>: не менее 10 139 ГБ; – <i>в архивах</i>⁴: не менее 30 417 ГБ. 5 000 EPS – <i>в оперативном доступе</i>: не менее 14 484 ГБ; – <i>в архивах</i>⁴: не менее 43 452 ГБ
Жесткий диск для хранения событий (LogSpace)	До 1000 Гб в оперативном доступе в общем случае.	До 2500 Гб в оперативном доступе в общем случае.
¹ Для установки ПО требуется не менее 800 ГБ эффективного объема дискового пространства в RAID-массиве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на SSD или HDD (10 000 об./мин.) SAS (рекомендуемая конфигурация RAID1+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями. Преобразовать файловую систему в ext4 (для Linux, размер блока 4096 байт). Дисковое пространство рекомендуется распределить между двумя разделами – объемом 200 ГБ для работы ОС (корневым каталогом / на Linux) и объемом не менее 600 ГБ для работы компонентов и баз данных (каталогом /var на Linux). ² Рекомендуется использовать отдельный RAID-массив (RAID1+1HS) для дисков типа SSD. Поддерживаемые конфигурации RAID-массивов приведены в Приложении Г и зависят от применяемых типов дисков. Рекомендуется при выборе конфигурации хранилища данных учитывать критерии масштабирования решений класса SIEM, такие как постепенное увеличение потока событий и увеличение сроков хранения событий в различном формате, что сказывается на расширении объема хранилища данных (конфигурация хранилища должна иметь возможность расширения сформированного объема с учетом выполнения требований по IOPS). ³ При сроках хранения событий в оперативном доступе – 30 дней рекомендуется рассчитывать объем дискового пространства для архивных событий – 90 дней. Сроки хранения могут быть изменены, определяются условиями применения ПК Ankey SIEM NG и описываются в проектных решениях. Внимание! Не следует превышать максимальный срок (90 суток) хранения событий в оперативном доступе Elasticsearch, т.к. если потребуется восстановить в оперативный доступ события из архивов, то максимальный срок в 90 суток будет превышен, что приведет к сбоям в работе Elasticsearch. На регулярной основе рекомендуется хранить в оперативном доступе события не более чем за 30 суток.		

⁴Архивные события должны храниться обязательно для восстановления, в случае необходимости, в оперативном доступе (срок хранения архивных событий не должен быть менее срока хранения событий, находящихся в оперативном доступе). Архивные данные могут быть размещены на выделенном дисковом RAID-массиве с дисками HDD (SAS/SATA от 7200 об./мин. и выше) или в RAID-массиве с SSD в случае выполнения требований по скорости восстановления систем (в зависимости от требований RTO для соответствующих объемов восстанавливаемых данных).

Хранилище для архивных событий должно быть больше, чем хранилище для событий в оперативном доступе минимум в 2 раза.

Примечание. Сроки хранения определяются проектными решениями: необходимо рассчитывать конфигурацию дискового хранилища в зависимости от сроков хранения пропорционально текущим значениям либо в зависимости от поступающего потока событий и среднего размера события (в расчет берутся как необработанные (RAW), так и нормализованные события).

Retro correlator. Требования

Таблица 3.2 – Аппаратные требования к серверу ретроспективной корреляции с компонентом Ankey SIEM NG Retro Correlator

Компонент сервера	Минимальное требование
Центральные процессоры	В процессоре(ах) должна быть реализована поддержка инструкций SSE4.2 и AVX и технология многопоточности, тактовая частота не менее 2,2 ГГц. В сумме не менее 8 логических ядер.
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый
Память (ОЗУ)	32 ГБ
Жесткие диски и свободное дисковое пространство для ОС и установки ПО ¹	не менее 1 000 ГБ ²
¹ Рекомендуется объединить жесткие диски в RAID-массив и преобразовать файловую систему в ext4 (для Linux, размер блока 4096 байт). ² Для установки ПО требуется не менее 1 000 ГБ эффективного объема дискового пространства в RAID-массиве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на HDD (10 000 об./мин.) SAS (рекомендуемая конфигурация RAID1+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями.	

3.2.3 Требования к аппаратному обеспечению конфигурации для средненагруженных систем

Компоненты ПК Ankey SIEM NG в конфигурации для средненагруженных систем необходимо устанавливать на серверы, которые соответствуют приведенным ниже требованиям к вычислительным ресурсам.

Core, MC, KB, Collector (до 15000 EPS, до 5000 активов). Требования

Таблица 3.3 – Аппаратные требования к серверу обработки и хранения с компонентами Ankey SIEM NG Server, Ankey SIEM NG Events Storage при общем потоке **до 10 000 событий в секунду** и общем количестве активов в СУБД Jatoba или PostgreSQL **до 3 500 единиц**

	Минимальные требования	
	До 10 000 событий в секунду (до 3 500 активов)	До 15 000 событий в секунду (до 5 000 активов)
Центральные процессоры	В процессоре(ах) должна быть реализована поддержка инструкций SSE4.2 и AVX и технология многопоточности, тактовая частота не менее 2,2 ГГц.	
Количество логических ядер в системе виртуализации	20	24
Память (ОЗУ)	36	48
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый	
Твердотельный накопитель для ОС и установки ПО	не менее 1 000 ГБ ¹	
¹ Для установки ОС и ПО требуется не менее 1 000 ГБ эффективного объема дискового пространства в RAID-массиве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на SSD (рекомендуемая конфигурация RAID10+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями. Рекомендуется преобразовать файловую систему в ext4 (для Linux, размер блока 4096 байт). Дисковое пространство рекомендуется распределить между двумя разделами – объемом 200 ГБ для работы ОС (корневым каталогом / на Linux) и объемом 800 ГБ для работы компонентов и баз данных (каталогом /var на Linux).		

Server, ES. Требования

Таблица 3.4 – Аппаратные требования к серверу обработки и хранения с компонентами Ankey SIEM NG Server, Ankey SIEM NG Events Storage при общем потоке **до 15 000 событий в секунду**

	Минимальные требования	
	До 10 000 событий в секунду	До 15 000 событий в секунду
Центральные процессоры	В процессоре(ах) должна быть реализована поддержка инструкций SSE4.2 и AVX и технология многопоточности, тактовая частота не менее 2,2 ГГц.	
Количество логических ядер в системе виртуализации	40	56
Память (ОЗУ)	112	128
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый	
Твердотельный накопитель для ОС и установки ПО	не менее 500 ГБ ¹	
Жесткий диск для хранения событий (Elasticsearch)	Расчетные значения³: 6 000 EPS в оперативном доступе: не менее 17 381 ГБ; в архивах⁴: не менее 52 143 ГБ. 7 000 EPS в оперативном доступе: не менее 20 278 ГБ; в архивах⁴: не менее 60 833 ГБ. 10 000 EPS в оперативном доступе: не менее 28 968 ГБ; в архивах⁴: не менее 86 904 ГБ	Расчетные значения³: 13 000 EPS в оперативном доступе: не менее 37 659 ГБ; в архивах⁴: не менее 112 975 ГБ. 14 000 EPS в оперативном доступе: не менее 40 556 ГБ; в архивах⁴: не менее 121 656 ГБ. 15 000 EPS в оперативном доступе: не менее 43 452 ГБ; в архивах⁴: не менее 130 356 ГБ
Жесткий диск для хранения событий (LogSpace)	До 5000 Гб в оперативном доступе в общем случае.	До 7500 Гб в оперативном доступе в общем случае.

Примечание. Чтобы определить требуемый объем свободного дискового пространства для хранения событий в оперативном доступе² и выбрать накопители для хранения событий (в компоненте Events Storage) следуйте инструкциям в пункте 3.2.7

¹ Для установки ОС и ПО требуется не менее 500 ГБ свободного места на дисковом пространстве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на SSD или HDD (10 000 об./мин.) SAS (рекомендуемая конфигурация RAID10+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями. Рекомендуется преобразовать файловую систему в ext4 (размер блока 4096 байт) и разделить дисковое пространство на три логических раздела – корневой каталог объемом 200 ГБ для работы ОС, каталог /var объемом 150 ГБ для файлов журналов ОС и RabbitMQ, каталог /opt объемом 150 ГБ для файлов журналов и кэша ПК Ankey SIEM NG.

² Рекомендуется использовать отдельный RAID-массив (RAID1+1HS) для дисков типа SSD. Поддерживаемые конфигурации RAID-массивов приведены в Приложении Г и зависят от применяемых типов дисков. Рекомендуется при выборе конфигурации хранилища данных учитывать критерии масштабирования решений класса SIEM, такие как постепенное увеличение потока событий и увеличение сроков хранения событий в различном формате, что сказывается на расширении объема хранилища данных (конфигурация хранилища должна иметь возможность расширения сформированного объема с учетом выполнения требований по IOPS).

³ При сроках хранения событий в оперативном доступе – 30 дней необходимо рассчитывать объем дискового пространства для архивных событий – 90 дней. Сроки хранения могут быть изменены, определяются условиями применения ПК Ankey SIEM NG и описываются в проектных решениях.

Внимание! Не следует превышать максимальный срок (90 суток) хранения событий в оперативном доступе Elasticsearch, т.к. если потребуется восстановить в оперативный доступ события из архивов, то максимальный срок в 90 суток будет превышен, что приведет к сбоям в работе Elasticsearch. На регулярной основе рекомендуется хранить в оперативном доступе события не более чем за 30 суток.

⁴ Архивные события должны храниться обязательно для восстановления, в случае необходимости, в оперативном доступе (срок хранения архивных событий не должен быть менее срока хранения событий, находящихся в оперативном доступе). Архивные данные могут быть размещены на выделенном дисковом RAID-массиве с дисками HDD (SAS/SATA от 7200 об./мин. и выше) или в RAID-массиве с SSD в случае выполнения требований по скорости восстановления систем (в зависимости от требований RTO для соответствующих объемов восстанавливаемых данных). Хранилище для архивных событий должно быть больше, чем хранилище для событий в оперативном доступе минимум в два раза.

Примечание. Сроки хранения определяются проектными решениями: необходимо рассчитывать конфигурацию дискового хранилища в зависимости от сроков хранения пропорционально текущим значениям либо в зависимости от поступающего потока событий и среднего размера события (в расчет берутся как необработанные (RAW), так и нормализованные события).

Retro correlator. Требования

Таблица 3.5 – Аппаратные требования к серверу ретроспективной корреляции с компонентом Ankey SIEM
NG Retro Correlator

Компонент сервера	Минимальное требование
Центральный процессор	В процессоре(ах) должна быть реализована поддержка инструкций SSE4.2 и AVX и технология многопоточности, тактовая частота не менее 2,2 ГГц. В сумме не менее 8 логических ядер.
Память (ОЗУ)	32 ГБ
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый
Жесткие диски и свободное дисковое пространство для ОС и установки ПО ¹	Жесткие диски и свободное дисковое пространство для ОС и установки ПО ²
¹ Рекомендуется объединить жесткие диски в RAID-массив и преобразовать файловую систему в ext4 (для Linux, размер блока 4096 байт). ² Для установки ПО требуется не менее 1 000 ГБ эффективного объема дискового пространства в RAID-массиве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на HDD (10 000 об./мин.) SAS (рекомендуемая конфигурация RAID1+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями.	

3.2.4 Требования к аппаратному обеспечению конфигурации для высоконагруженных систем

Компоненты ПК Ankey SIEM NG в конфигурации для высоконагруженных систем необходимо устанавливать на серверы, которые соответствуют приведенным ниже требованиям к вычислительным ресурсам.

Core, MC, KB (до 300.000 EPS). Требования

Таблица 3.6 – Аппаратные требования к серверу управления с компонентами Ankey SIEM NG Core, Ankey SIEM NG MC и Ankey SIEM NG Knowledge Base при общем потоке **до 300 000 событий в секунду** и общем количестве активов в СУБД Jatoba или PostgreSQL до 100.000¹⁴

	Минимальные требования			
	До 30 000 событий в секунду (до 10 000 активов)	До 50 000 событий в секунду (до 20 000 активов)	До 100 000 событий в секунду ¹⁵ (до 30 000 активов ¹⁶)	До 300 000 событий в секунду ¹⁵ (до 100 000 активов ¹⁶)
Центральные процессоры	В процессоре(ах) должна быть реализована поддержка инструкций SSE4.2 и AVX и технология многопоточности, тактовая частота не менее 2,2 ГГц.			
Количество логических ядер в системе виртуализации	32	32	48	64
Память (ОЗУ)	64ГБ	64ГБ	96ГБ	128ГБ
Сетевой адаптер	2 порта со скоростью 10 Гбит/с каждый			
Твердотельный накопитель для ОС и установки ПО. Общий объём.	не менее 1 000 ГБ ¹ эффективного объема дискового пространства в RAID-массиве	не менее 1 500 ГБ ¹ эффективного объема дискового пространства в RAID-массиве	не менее 2 500 ГБ ¹ эффективного объема дискового пространства в RAID-массиве	не менее 5 000 ГБ ¹ эффективного объема дискового пространства в RAID-массиве
для работы компонентов и баз данных (каталог /var на Linux).	800 ГБ	1 300 ГБ	2 300 ГБ	4 800 ГБ

¹⁴ Превышение количества активов свыше 100.000 возможно, однако разработчик не гарантирует стабильную работу такой конфигурации.

¹⁵ При развертывании нескольких конвейеров Ankey SIEM NG

¹⁶ В случае, если количество хранимых в Core активов превышает 20 000, необходимо увеличить объем вычислительных ресурсов (CPU, HDD, RAM), которые требуются для функционирования Core

для работы ОС (корневой каталог / на Linux),	200 ГБ
¹ Для повышения отказоустойчивости при любой конфигурации рекомендуется использовать отдельный RAID на SSD (рекомендуемая конфигурация RAID10+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями. Рекомендуется преобразовать файловую систему в ext4 (для Linux, размер блока 4096 байт)	

Server (до 50.000 событий). Требования

Таблица 3.7 – Аппаратные требования к серверу обработки с компонентом Ankey SIEM NG Server при общем потоке **до 50 000** событий

	Минимальные требования			
	До 20 000 событий	До 30 000 событий	До 40 000 событий	До 50 000 событий
Центральные процессоры	В процессоре(ах) должна быть реализована поддержка инструкций SSE4.2 и AVX и технология многопоточности, тактовая частота не менее 2,2 ГГц.			
Количество логических ядер в системе виртуализации	32	32	48	64
Память (ОЗУ)	64Гб	64Гб	96Гб	128Гб
Сетевой адаптер	2 порта со скоростью 10 Гбит/с каждый			
Твердотельный накопитель для ОС и установки ПО. Общий объём.	не менее 1 000 ГБ ¹			
для работы компонентов и баз данных (каталог /var на Linux).	400 ГБ			
для работы ОС (корневой каталог / на Linux),	200 ГБ			
для файлов журналов и кэша ПК Ankey SIEM NG (каталог /opt)	400 ГБ			
¹ Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на SSD (рекомендуемая конфигурация RAID10+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями. Преобразовать файловую систему в ext4 (размер блока 4 096 байт) и разделить дисковое пространство на три логических раздела – корневой каталог для работы ОС, каталог /var для файлов журналов ОС и RabbitMQ, каталог /opt для файлов журналов и кэша ПК Ankey SIEM NG.				

Events Storage (до 50 000 событий в секунду). Требования

Таблица 3.8 – Аппаратные требования к серверу хранения с компонентом Ankey SIEM NG Events Storage
(с хранилищем **Elasticsearch**)

	Минимальные требования			
	До 20 000 событий в секунду	До 30 000 событий в секунду	До 40 000 событий в секунду	До 50 000 событий в секунду
Количество логических ядер в системе виртуализации	28	36	52	60
Память (ОЗУ)	160 ГБ	192 ГБ	192 ГБ	256 ГБ
Твердотельный накопитель (SSD) для системных данных	Не менее 500 ГБ ¹			
Сетевой адаптер	2 порта со скоростью 10 Гбит/с каждый			
Твердотельный накопитель (SSD) для хранения индексов в горячей стадии	до 6 000 ГБ	до 8 000 ГБ	до 12 000 ГБ	до 14 000 ГБ
Жесткий диск (HDD) для хранения индексов в теплой стадии Примечание. Чтобы определить требуемый объем свободного дискового пространства для хранения событий в оперативном доступе ² и выбрать накопителя для хранения событий (в компоненте Events Storage) следуйте инструкциям в пункте 3.2.7	<u>Расчетные значения</u> ³ : 10 000 EPS – в оперативном доступе: не менее 38 624 ГБ; – в архивах ⁴ : не менее 115 872 ГБ. 15 000 EPS – в оперативном доступе: не менее 43 452 ГБ; – в архивах: не менее 115 872 ГБ. 20 000 EPS – в оперативном доступе:	<u>Расчетные значения</u> ³ : 25 000 EPS – в оперативном доступе: не менее 72 419 ГБ; – в архивах ⁴ : не менее 217 258 ГБ 30 000 EPS – в оперативном доступе: не менее 86 903 ГБ; в архивах: не менее 260 710 ГБ	<u>Расчетные значения</u> ³ : 35 000 EPS – в оперативном доступе: не менее 101 387 ГБ; – в архивах ⁴ : не менее 304 162 ГБ 40 000 EPS – в оперативном доступе: не менее 115 872 ГБ; в архивах: не менее 347 615 ГБ	<u>Расчетные значения</u> ³ : 45 000 EPS – в оперативном доступе: не менее 130 356 ГБ; – в архивах ⁴ : не менее 391 067 ГБ 50 000 EPS – в оперативном доступе: не менее 144 840 ГБ; в архивах: не менее 434 518 ГБ

	не менее 57 936 ГБ; – в архивах: не менее 173 808 ГБ.			
¹ Для установки ПО требуется не менее 500 ГБ свободного места на дисковом пространстве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на SSD или HDD (10000 об./мин.) SAS (рекомендуемая конфигурация RAID1+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями. Преобразовать файловую систему в ext4 (размер блока 4096 байт) и разделить дисковое пространство на два логических раздела – корневой каталог объемом 200 ГБ для работы ОС и каталог <code>/es_logs</code> объемом 300 ГБ для файлов журналов Ankey SIEM NG Events Storage. ² Рекомендуется использовать отдельный RAID-массив (RAID10+1HS) для дисков типа SSD. Поддерживаемые конфигурации RAID-массивов приведены в Приложении Г и зависят от применяемых типов дисков. Рекомендуется при выборе конфигурации хранилища данных учитывать критерии масштабирования решений класса SIEM, такие как постепенное увеличение потока событий и увеличение сроков хранения событий в различном формате, что сказывается на расширении объема хранилища данных (конфигурация хранилища должна иметь возможность расширения сформированного объема с учетом выполнения требований по IOPS). ³ При сроках хранения событий в оперативном доступе – 30 дней необходимо рассчитывать объем дискового пространства для архивных событий – 90 дней. Сроки хранения могут быть изменены, определяются условиями применения ПК Ankey SIEM NG и описываются в проектных решениях. Внимание! Не следует превышать максимальный срок (90 суток) хранения событий в оперативном доступе Elasticsearch, т.к. если потребуется восстановить в оперативный доступ события из архивов, то максимальный срок в 90 суток будет превышен, что приведет к сбоям в работе Elasticsearch. На регулярной основе рекомендуется хранить в оперативном доступе события не более чем за 30 суток. ⁴ Архивные события должны храниться обязательно для восстановления, в случае необходимости, в оперативном доступе (срок хранения архивных событий не должен быть менее срока хранения событий, находящихся в оперативном доступе). Архивные данные могут быть размещены на выделенном дисковом RAID-массиве с дисками HDD (SAS/SATA от 7200 об./мин. и выше) или в RAID-массиве с SSD в случае выполнения требований по скорости восстановления систем (в зависимости от требований RTO для соответствующих объемов восстанавливаемых данных). Хранилище для архивных событий должно быть больше, чем хранилище для событий в оперативном доступе минимум в два раза. Примечание. Сроки хранения определяются проектными решениями: необходимо рассчитывать конфигурацию дискового хранилища в зависимости от сроков хранения пропорционально текущим значениям либо в зависимости от поступающего потока событий и среднего размера события (в расчет берутся как необработанные (RAW), так и нормализованные события).				

Таблица 3.9 – Аппаратные требования к серверу хранения с компонентом Ankey SIEM NG Events Storage
(с хранилищем **Logspace**)

	Минимальные требования			
	До 20 000 событий в секунду	До 30 000 событий в секунду	До 40 000 событий в секунду	До 50 000 событий в секунду
Количество логических ядер в системе виртуализации	14	16	20	24
Память (ОЗУ)	96 ГБ	96 ГБ	128 ГБ	192 ГБ
Твердотельный накопитель (SSD) для системных данных	Не менее 500 ГБ ¹			
Жесткий диск (HDD) для хранения событий	10 000 ГБ	15 000 ГБ	20 000 ГБ	24 000 ГБ
Примечание. Чтобы определить требуемый объем свободного дискового пространства для хранения событий в оперативном доступе ² и выбрать накопители для хранения событий (в компоненте Events Storage) следуйте инструкциям в пункте 3.2.7				
Сетевой адаптер	2 порта со скоростью 10 Гбит/с каждый			

¹ Для установки ПО требуется не менее **500 ГБ** свободного места на дисковом пространстве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на SSD или HDD (10000 об./мин.) SAS (рекомендуемая конфигурация RAID1+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями. Преобразовать файловую систему в ext4 (размер блока 4096 байт) и разделить дисковое пространство на два логических раздела – корневой каталог объемом **200 ГБ** для работы ОС и каталог /es_logs объемом **300 ГБ** для файлов журналов Ankey SIEM NG Events Storage.

² Рекомендуется использовать отдельный RAID-массив (RAID10+1HS) для дисков типа SSD. Поддерживаемые конфигурации RAID-массивов приведены в Приложении Г и зависят от применяемых типов дисков. Рекомендуется при выборе конфигурации хранилища данных учитывать критерии масштабирования решений класса SIEM, такие как постепенное увеличение потока событий и увеличение сроков хранения событий в различном формате, что сказывается на расширении объема хранилища данных (конфигурация хранилища должна иметь возможность расширения сформированного объема с учетом выполнения требований по IOPS).

³ При хранении событий за 30 дней и среднем размере события 1—2 КБ, а также сохранении сырых и нормализованных данных о событиях. Рекомендуется использовать жесткие диски (HDD) со скоростью вращения 7200 об./мин каждый, объединенные в массив RAID 10, создать раздел с файловой системой ext4 (размер блока 4096 байт) объемом не менее указанного в таблице и смонтировать его как каталог для хранения событий (по умолчанию /opt/logspaced).

Retro correlator. Требования

Таблица 3.10 – Аппаратные требования к серверу ретроспективной корреляции с компонентом Ankey SIEM
NG Retro Correlator

Компонент сервера	Минимальное требование
Центральный процессор	В процессоре(ах) должна быть реализована поддержка инструкций SSE4.2 и AVX и технология многопоточности, тактовая частота не менее 2,2 ГГц. В сумме не менее 8 логических ядер.
Память (ОЗУ)	32 ГБ
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый
Жесткие диски и свободное дисковое пространство для ОС и установки ПО ¹	Жесткие диски и свободное дисковое пространство для ОС и установки ПО ²
¹ Рекомендуется объединить жесткие диски в RAID-массив и преобразовать файловую систему в ext4 (для Linux, размер блока 4096 байт). ² Для установки ПО требуется не менее 1 000 ГБ эффективного объема дискового пространства в RAID-массиве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на HDD (10 000 об./мин.) SAS (рекомендуемая конфигурация RAID1+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями.	

3.2.5 Аппаратные требования к серверу сбора событий с компонентом Ankey SIEM NG Collector, размещенному в отдельном сегменте сети

Компонент Ankey SIEM NG Collector, размещенный в отдельном сегменте сети, необходимо устанавливать на серверы, удовлетворяющие приведенным ниже аппаратным требованиям. Данные аппаратные требования актуальны для всех типов конфигураций системы.

Таблица 3.11 – Аппаратные требования к серверу сбора событий с компонентом Ankey SIEM NG Collector, размещенному в отдельном сегменте сети, который предназначен **для сбора событий**.

Компонент сервера	Минимальные требования			
	До 500 событий\сек.	До 1 500 событий\сек.	До 5 000 событий\сек.	До 15 000 событий\сек. ³
Центральные процессоры	В процессоре(ах) должна быть реализована поддержка инструкций SSE4.2 и AVX и технология многопоточности, тактовая частота не менее 2,2 ГГц.			
Количество логических ядер в системе виртуализации	6	8	12	16
Память (ОЗУ)	6 ГБ	8 ГБ	12 ГБ	24 ГБ
Сетевой адаптер	2 порта со скоростью 10 Гбит/с каждый			
Жесткие диски и свободное дисковое пространство для ОС и установки ПО ¹	не менее 300 ГБ эффективного объема дискового пространства в RAID-массиве ² .			

¹ Рекомендуется преобразовать файловую систему в ext4 (для Linux, размер блока 4096 байт).

² Для ОС и установки ПО требуется не менее 300 ГБ свободного дискового пространства. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на HDD (10 000 об./мин.) SAS (рекомендуемая конфигурация RAID1+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями.

³ Не более 5000 событий в секунду на одну задачу по сбору событий. Максимальный поток событий в секунду для компонента Ankey SIEM NG Collector может быть увеличен в конфигурациях для высоконагруженных систем с учетом развития функциональных возможностей (по потоку событий) компонентов платформы. Рекомендуется использовать данные вычислительные ресурсы для сервера компонента Ankey SIEM NG Collector в тех случаях, когда невозможно развернуть несколько серверов сбора событий на одном объекте и общий поток событий на объекте может превысить 5 000 событий в секунду (с учетом возникновения всплесков событий от среднего потока).

Примечание. Максимальное количество одновременно функционирующих задач с модулями опроса конфигураций (аудита) активов ограничено. На одном коллекторе не рекомендуется одновременно запускать: более 4 задач с каждым модулем audit, pentest, customeventcollector, vshperevenetcollector; более 100 задач с модулями syslog, wineventlog, filemonitor, netflow, odbclog, networkwatch, ssheventcollector, snmpeventcollector; более 1 задачи с каждым модулем hostdiscovery, batcheventsearch, dpicollector, mp8scanimporter.

Таблица 3.12 – Аппаратные требования к серверу сбора событий с компонентом Ankey SIEM NG Collector, размещенному в отдельном сегменте сети, который предназначен **для сканирования активов**.

Компонент сервера	Минимальное требование		
	Конфигурации для низконагруженных систем. 4 потока сканирования модулями Audit и Pentest на один коллектор	Конфигурации для средненагруженных систем. 10 потоков сканирования модулями Audit и Pentest на один коллектор	Конфигурации для высоконагруженных систем. 20 потоков сканирования модулями Audit и Pentest на один коллектор
Центральные процессоры	В процессоре(ах) должна быть реализована поддержка инструкций SSE4.2 и AVX и технология многопоточности, тактовая частота не менее 2,2 ГГц.		
Количество логических ядер в системе виртуализации	4	6	8
Память (ОЗУ)	4 ГБ	8 ГБ	12 ГБ
Сетевой адаптер	2 порта со скоростью 10 Гбит/с каждый		
Жесткие диски и свободное дисковое пространство для ОС и установки ПО ¹	не менее 300 ГБ эффективного объема дискового пространства в RAID-массиве ² .		
¹ Рекомендуется преобразовать файловую систему в ext4 (для Linux, размер блока 4096 байт).			
² Для ОС и установки ПО требуется не менее 300 ГБ свободного дискового пространства. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на HDD (10 000 об./мин.) SAS (рекомендуемая конфигурация RAID1+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями.			

Примечание. Максимальное количество одновременно функционирующих задач с модулями опроса конфигураций (аудита) активов ограничено. На одном коллекторе не рекомендуется одновременно запускать: более 4 задач с каждым модулем audit, pentest, customeventcollector, vshperevenetcollector; более 100 задач с модулями syslog, wineventlog, filemonitor, netflow, odbclog, networkwatch, ssheventcollector, snmpeventcollector; более 1 задачи с каждым модулем hostdiscovery, batcheventsearch, dpicollector, mp8scanimporter.

3.2.6 Аппаратные требования к серверу облегченной версии Ankey SIEM NG Server («SIEM на коллекторе»)

Компоненты Ankey SIEM NG Collector и Ankey SIEM NG Server в конфигурации облегченная версия Ankey SIEM NG Server («SIEM на коллекторе») необходимо устанавливать на серверы, которые соответствуют приведенным ниже требованиям к вычислительным ресурсам.

Данные требования к вычислительным ресурсам для «SIEM на коллекторе» актуальны для всех конфигураций ПК Ankey SIEM NG.

Таблица 3.13 – Аппаратные требования к серверу сбора и обработки событий с компонентами Ankey SIEM NG Collector и Ankey SIEM NG Server («SIEM на коллекторе»)

Компонент сервера	Минимальное требование
Центральный процессор	В процессоре(ах) должна быть реализована поддержка инструкций SSE4.2 и AVX и технология многопоточности, тактовая частота не менее 2,2 ГГц. В сумме не менее 56 логических ядер.
Память (ОЗУ)	64 ГБ
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый
Жесткие диски и свободное дисковое пространство	Для ОС и установки ПО: диски HDD (10000 об./мин.) SAS или SSD не менее 2 000 ГБ эффективного объема дискового пространства в RAID-массиве ¹
¹ Для установки ОС и ПО требуется не менее 2 000 ГБ свободного места на дисковом пространстве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на HDD (10 000 об./мин.) SAS (рекомендуемая конфигурация RAID1+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями.	

3.2.7 Рекомендации по расчету объема и выбору накопителей для хранения событий

Примечание. Рекомендуемые конфигурации для систем хранения событий информационной безопасности представлены в приложении Г.

Для определения требуемого объема свободного дискового пространства необходимо выполнить расчеты.

Примечание. Расчеты выполняются для определения объема требуемого дискового пространства для необработанных и обработанных событий.

Вы можете рассчитать приблизительный объем (в байтах), необходимый для хранения суточного объема данных о событиях, по формуле:

$V_{hdd} = R \cdot T \cdot EPS$, где

V_{hdd} – объем свободного дискового пространства;

EPS – (events per second) суммарное количество событий ИБ в секунду от всех источников событий;

R – средний размер события ИБ в байтах:

- 1 200 байт – при использовании хранилища Elasticsearch;
- 200 байт – при использовании хранилища Logspace.

T – количество секунд в сутках ($3600 \times 24 = 86\,400$ секунд);

Например, при средней скорости 1 000 событий в секунду система запишет за сутки $1\,200 \times 86\,400 \times 1\,000 \approx 104$ ГБ данных, если используется хранилище Elasticsearch.

Объем требуемого дискового пространства для хранения событий ИБ на определенном периоде времени рассчитывается по формуле:

$V_{hdd} = EPS \cdot R \cdot T / (1024 \cdot 1024 \cdot 1024) \cdot D$, где

V_{hdd} – объем свободного дискового пространства;

EPS – (events per second) суммарное количество событий ИБ в секунду от всех источников событий;

R – средний размер события ИБ в байтах:

- 1 200 байт – при использовании хранилища Elasticsearch;
- 200 байт – при использовании хранилища Logspace.

T – количество секунд в сутках (86400 секунд);

$1024 \cdot 1024 \cdot 1024$ – перевод из байтов в Гигабайты;

D – общее количество дней, в течение которых требуется хранить события ИБ.

Пример расчета объема дискового пространства для хранения событий в течение 30 дней при суммарном потоке 50 000 событий в секунду:

$V_{hdd} = 50\,000 \times 1\,200 \times 86\,400 / (1024 \times 1024 \times 1024) \times 30 \approx 144\,839$ ГБ, , если используется хранилище Elasticsearch.

Реальное потребление свободного места зависит от типа событий. Может быть как меньше, так и больше значений, рассчитанных по формуле.

В низконагруженной конфигурации рекомендуется объединить жесткие диски или твердотельные диски в массив RAID 10 и выделить на отдельном логическом диске каталог /data для хранения индексов в оперативном доступе с событиями информационной безопасности. Для организации хранения архивных индексов необходимо выделить дополнительный логический диск для

каталога `/es_backup`¹⁷ (описание создания хранилища индексов представлено в Руководстве администратора Ankey SIEM NG 5.2.3).

В средненагруженной и высоконагруженной (с потоком событий до 20000 в секунду) конфигурациях рекомендуется объединить жесткие диски или твердотельные диски в массив RAID 10 и выделить в отдельную файловую систему каталог `/data` для хранения индексов в оперативном доступе с событиями информационной безопасности. Для организации хранения архивных индексов необходимо выделить в отдельную файловую систему каталог `/es_backup`¹⁷. Объем дискового пространства для архивных индексов зависит от объема индексов в оперативном доступе и необходимого срока хранения.

В высоконагруженной (с потоком событий более 20000 в секунду) конфигурации необходимо использовать два типа накопителей данных: жесткие диски и твердотельные накопители. Рекомендуется объединить жесткие диски в массив RAID 10 и подключить к ним каталог `/data` для хранения индексов, находящихся в «теплой» стадии, твердотельные накопители – объединить в массив RAID 6 и подключить к ним каталог `/datahot` для хранения индексов, находящихся в «горячей» стадии.

Примечание. Подробное описание стадий жизненного цикла индексов приведено на сайте elastic.co.

3.2.8 Рекомендации по развертыванию ПК Ankey SIEM NG в виртуальной среде

Внимание! Не используйте динамическую миграцию виртуальных машин для сервера Ankey SIEM NG Core, например VMware vSphere vMotion, так как после каждой миграции необходимо повторно активировать лицензию на Ankey SIEM NG.

Рекомендуется использовать версию 11 виртуальной машины VMware vSphere и версию 6.0 гипервизора VMware ESXi с приведенными ниже параметрами распределения ресурсов.

Настройка гипервизора

Рекомендуется использовать технологию Storage I/O Control при обмене данными между гипервизором и хранилищами, содержащими виртуальные машины, на которых будут развернуты компоненты системы.

Для закрепления за виртуальной машиной выделенных для нее аппаратных ресурсов (например, логических ядер) рекомендуется в параметрах виртуальной машины **VM Options** → **Advanced** в раскрывающемся списке **Latency Sensitivity** выбрать **High**. Для каждой такой виртуальной машины нужно дополнительно оставлять два свободных логических ядра.

¹⁷ При установке можно задать пользовательское наименование каталога (например: `/data_archive`). Подробнее см. пункт 3.10.2.

Настройка центрального процессора

В аппаратных требованиях к центральному процессору указано минимальное количество логических ядер. Если сервер гипервизора использует технологию Hyperthreading, виртуальной машине достаточно выделить вдвое меньше физических ядер. Если технология Hyperthreading не используется, количество выделенных физических ядер должно быть равно количеству логических. Например, если виртуальной машине требуется 56 логических ядер и сервер гипервизора использует технологию Hyperthreading, виртуальной машине достаточно выделить два процессора по 14 ядер каждый.

Для повышения производительности виртуальной машины рекомендуется в блоке параметров **Hyperthreaded Core Sharing** выбрать режим **None**, в блоке параметров **Resource Allocation** передвинуть максимально вправо ползунок **Reservation** и установить флажок **Unlimited**.

Настройка BIOS

Для исключения задержек при выходе ядер процессора из спящего режима рекомендуется выбрать в параметрах BIOS производительный режим работы системы (профиль Performance в серверах компании Dell или аналогичные профили в серверах других производителей).

Для повышения производительности ядер процессоров, поддерживающих технологию Intel Turbo Boost, рекомендуется включить в системных параметрах BIOS использование этой технологии.

Настройка оперативной памяти

Объем оперативной памяти, выделяемой каждой виртуальной машине, не должен быть меньше значения, указанного в аппаратных требованиях. Также необходимо учитывать, что часть оперативной памяти сервера (до 8% от общего объема) должна быть зарезервирована для работы гипервизора.

Для работы виртуальной машины рекомендуется зарезервировать постоянный объем оперативной памяти, установив в блоке параметров **Resources Allocation** флажок **Reserve all guest memory (All locked)**.

Настройка виртуальных жестких дисков

Объем и производительность виртуальных жестких дисков не должны быть меньше значений, указанных в аппаратных требованиях.

При создании виртуального жесткого диска на шаге **Create a Disk** в блоке параметров **Disk Provisioning** рекомендуется выбрать вариант **Thick Provision Eager Zeroed**, на шаге **Advanced Options** в блоке параметров **Mode** рекомендуется установить флажок **Independent**, а затем выбрать вариант **Persistent**.

3.2.9 Взаимодействие с внешними системами

Средства обеспечения безопасности могут оказывать влияние на работу ПК Ankey SIEM NG. Поэтому на этапе планирования и развертывания рекомендуется провести тестовые сканирования и при необходимости принять меры для снижения негативных последствий. Например, может потребоваться отключить средства межсетевого экранирования, антивирусную защиту или специализированные средства контроля аппаратного оборудования на серверах, где установлены компоненты ПК Ankey SIEM NG.

Большинство сетевых средств обеспечения безопасности содержат модули анализа прикладных протоколов (stateful inspection, application firewall), которые могут вмешиваться в процесс сканирования, снижая достоверность полученных результатов. Так, например, результат сканирования веб-приложения через межсетевой экран, поддерживающий функции защиты веб-приложений (web application firewall), не будет достоверным, поскольку межсетевой экран заблокирует ряд потенциально опасных запросов, используемых сканером. В некоторых средствах защиты нельзя отключить фильтрацию прикладных протоколов для отдельных узлов, и в таких случаях рекомендуется выносить Ankey SIEM NG Collector за межсетевой экран.

Системы обнаружения и предотвращения атак часто реагируют на процесс сканирования как на потенциальную атаку. Получение списка открытых портов, проверка стойкости паролей, доступ к протоколам удаленного управления – все это может привести к срабатыванию средств защиты. В случае, если механизм предотвращения атак не задействован, множественные срабатывания сигнатур приведут только к увеличению объема журналов системы обнаружения атак. Если механизм предотвращения атак включен, то система может вмешаться в процесс сканирования и исказить результаты работы. В связи с этим рекомендуется вносить узлы, на которых установлены компоненты ПК Ankey SIEM NG, в список исключений системы обнаружения атак.

3.3 Подготовка к развертыванию Ankey SIEM NG

Перед установкой Ankey SIEM NG на любые ОС необходимо:

- проверить, что все серверы соответствуют аппаратным и программным требованиям;
- в качестве адресов компонентов Ankey SIEM NG на узлах использовать только IP-адреса или только FQDN. Использование двух способов адресации приводит к ошибкам при развертывании системы;

Примечание. При использовании NAT в ИТ-инфраструктуре организации рекомендуется использовать в качестве адресов компонентов только FQDN.

- при использовании FQDN в качестве адресов компонентов Ankey SIEM NG на узлах необходимо настроить и обеспечить доступность DNS для корректного разрешения имен узлов в IP-адреса;

Внимание! Не рекомендуется вносить изменения в файл `/etc/hosts`. Этот файл не используется компонентами Ankey SIEM NG.

- синхронизировать дату и время на серверах, на которые будут установлены компоненты;
- проверить, что в ОС серверов нет учетных записей с логином `siem`;

Внимание! Логин учетной записи `siem` зарезервирован Ankey SIEM NG. Не создавайте в операционной системе учетные записи с логином `siem`, так как это сделает установку Ankey SIEM NG невозможной.

- при установке или обновлении операционной системы – указать в качестве используемого формата размещения таблиц разделов на физическом жестком диске стандарт GPT.

Для установки Ankey SIEM NG используются полные доменные имена серверов (FQDN), поэтому перед началом развертывания рекомендуется убедиться, что в выводе команды `hostnamectl` для каждого сервера в строке `Static hostname` содержится корректный FQDN.

Примечание. При развертывании компонента Ankey SIEM NG Collector устанавливается драйвер WinPcap 4.1.3. Не рекомендуется дополнительно устанавливать другие версии драйвера WinPcap, поскольку работа другой версии драйвера может привести к некорректной работе модуля `hostdiscovery`.

3.4 Об установке компонентов на Linux с помощью ролей

Роль является базовой единицей развертывания на Linux и представляет собой совокупность служб, утилит и сценариев, обеспечивающих работу определенного набора функций системы. Каждая роль поставляется в виде отдельного архива, который может содержать Docker-образы или deb-пакеты.

При развертывании системы создаются экземпляры ролей, которые распределяются по приложениям определенного типа (Management and Configuration, Knowledge Base или Ankey SIEM NG). Такая архитектура позволяет гибко и удобно развертывать систему, а также обновлять и настраивать ее в дальнейшем. Тип приложения определяется составом входящих в него экземпляров ролей:

- приложение Management and Configuration содержит только роли `SqlStorage/JatobaStorage` и `Management and Configuration`;
- приложение Knowledge Base – только роль `Knowledge Base`;
- приложение Ankey SIEM NG – только роли `Core`, `SIEM Server`, `Events Storage Elasticsearch` (с хранилищем данных

Elasticsearch), Events Storage LogSpace¹⁸ (с хранилищем данных LogSpace), Collector, RMQ Message Bus и Retro Correlator.

Примечание. При разворачивании системы можно создать несколько приложений одного типа (например, несколько приложений Management and Configuration), однако такие конфигурации не поддерживаются производителем.

Управление разворачиванием обеспечивается ролью Deployer, которая построена на базе системы управления конфигурациями SaltStack. Ее модуль Salt Master обеспечивает общее управление установкой (созданием экземпляров) ролей, модули Salt Minion – установку ролей на каждый сервер системы.

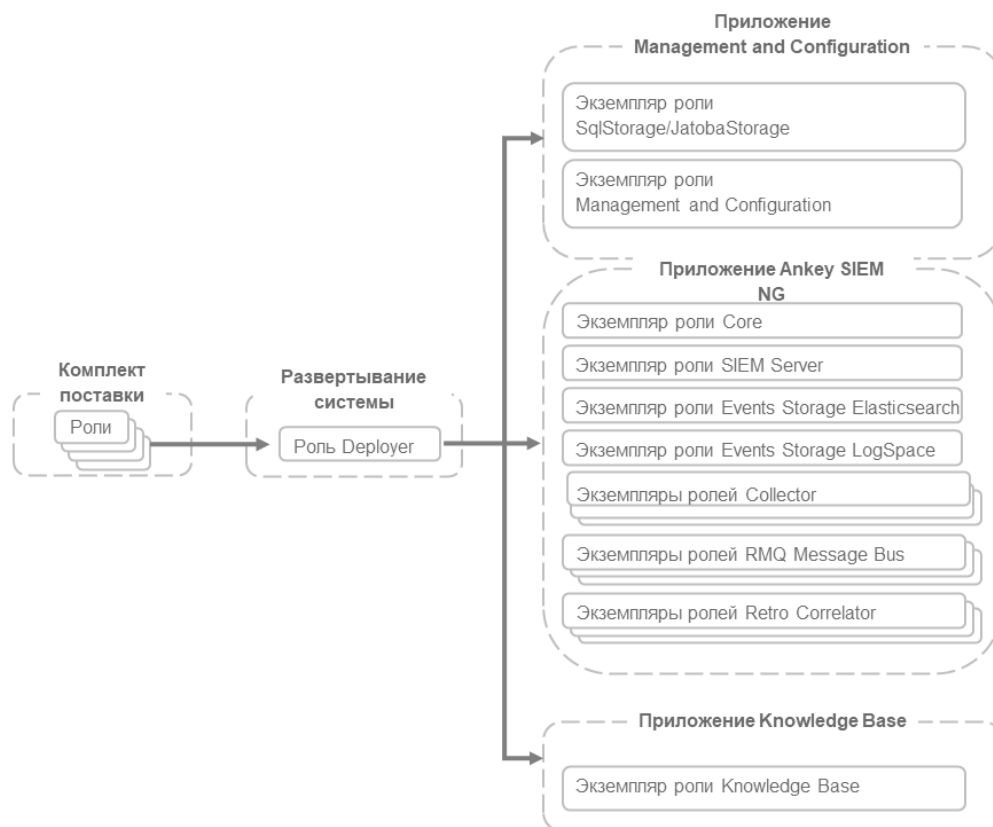


Рисунок 3.13 – Развертывание системы с помощью ролей

Для установки компонента может потребоваться установка как одной, так и нескольких ролей. В общем случае установка роли делится на следующие этапы:

1. Распаковка архива и запуск сценария установки.
2. Выбор приложения для установки роли. Вам потребуется или выбрать ранее созданное приложение необходимого типа, или создать новое, если приложение необходимого типа отсутствует.

¹⁸ Функциональные ограничения хранилища данных LogSpace описаны в подразделе 3.10.

При создании приложения нужно ввести его идентификатор, который среди прочего будет использоваться в качестве имени каталога для размещения файлов всех экземпляров ролей, входящих в состав данного приложения.

Примечание. Вы можете использовать идентификаторы, предлагаемые системой по умолчанию. Например, если для приложения Management and Configuration использовать предлагаемый по умолчанию идентификатор mc-application-ankey, файлы всех экземпляров ролей этого приложения будут размещены в каталоге /var/lib/deployed-roles/mc-application-ankey.

3. Ввод названия экземпляра роли и выбор сервера для ее установки. Введенное название среди прочего будет использоваться в качестве имени каталога для размещения файлов создаваемого экземпляра роли (например, файлов журналов и файлов конфигурации).

Примечание. Вы можете использовать названия, предлагаемые системой по умолчанию. Например, если для роли Collector использовать предлагаемое по умолчанию название agentlinux, файлы этого экземпляра ролей будут размещены в каталоге /var/lib/deployed-roles/ankey-application/agentlinux/ (шаблонный вид пути – /var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли %Компонент%>).

4. Проверка и изменение параметров конфигурации.
5. Запуск установки.

В результате установки роли (в том числе и неуспешной), в каталоге, из которого был запущен сценарий install.sh, формируется каталог installReports с отчетами об установке. Отчет сохраняется в HTML-файле и содержит данные о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

3.5 Сценарий развертывания ПК Ankey SIEM NG

Компоненты Ankey SIEM NG Core, Ankey SIEM NG MC, Knowledge Base, Ankey SIEM NG Server и Ankey SIEM NG Events Storage устанавливаются на Linux. При такой установке базовыми единицами развертывания являются роли (см. подраздел 3.4).

Внимание! Все установочные файлы ПК Ankey SIEM NG¹⁹ следует разместить в соответствии со структурой и порядком каталогов на хосте, где планируется установка компонента Core. Весь процесс установки ролей компонентов ПК Ankey SIEM NG необходимо выполнять с хоста, где планируется установка роли Deployer. Все операции должны выполняться с правами суперпользователя (root).

Внимание! Примеры распределения ролей и порядка действий по серверам ПК Ankey SIEM NG в зависимости от выбранной конфигурации представлены в приложении А.

При развертывании необходимо придерживаться следующего порядка действий²⁰:

1. Установить и настроить ОС Astra Linux Special Edition 1.7.5 или Debian 10.3 – 10.13. Подробнее см. [инструкцию по установке ОС Astra Linux Special Edition 1.7.5](#) или инструкцию по установке Debian 10.3 – 10.13, а также подраздел 3.3 «Рекомендации к установке ПК Ankey SIEM NG на ОС Astra Linux SE».
2. Установка роли Deployer (см. подраздел 3.6).
3. Установка компонента Ankey SIEM NG MC (см. подраздел 3.7):
 - 3.1 Установка роли SqlStorage (см. пункт 3.7.1) или JatobaStorage (см. пункты 3.7.3 или 3.7.4).
 - 3.2 Установка роли Management and Configuration (см. пункт 3.7.5).
4. Установка компонента Knowledge Base (см. подраздел 3.8):
 - 4.1 Установка роли Knowledge Base.
5. Установка компонента Ankey SIEM NG Core (см. подраздел 3.9):
 - 5.1 Установка роли RMQ Message Bus на сервер Ankey SIEM NG Core (см. пункт 3.9.1).
 - 5.2 Установка роли Core (см. пункт 3.9.2).
6. Установка компонента Ankey SIEM NG Events Storage (см. подраздел 3.10):

¹⁹ Если реализована поставка ПК Ankey SIEM NG на нескольких носителях (например, в виде компакт-дисков), то необходимо перенести установочные файлы со всех носителей в среду функционирования для последующего запуска установки ПО в соответствующей конфигурации. При копировании дополнительного ПО на хост следует выполнять копирование архивов, а не каталогов. Копирование каталогов с дополнительным ПО может привести к перезаписи содержимого уже существующих каталогов на хосте. Т.е. в уже готовую структуру каталогов с основным ПО Ankey SIEM NG на хосте необходимо добавить только архивы с дополнительным ПО.

²⁰ Все команды далее в терминале необходимо выполнять с правами суперпользователя root. Для этого можно перейти в учетную запись суперпользователя с помощью команды `sudo -s` или выполнять команды под учетной записью текущего пользователя используя команду `sudo` (например, `sudo ./install.sh`).

- 6.1 Установка модуля Salt Minion на сервер Ankey SIEM NG Events Storage²¹ (см. пункт 3.10.1).
- 6.2 Установка роли Event Storage с хранилищем событий Elasticsearch (см. пункт 3.10.2).
- 6.3 Установка роли Event Storage с хранилищем событий LogSpace (опционально) (см. пункт 3.10.3).
7. Установка компонента Ankey SIEM NG Server (см. подраздел 3.11).
 - 7.1 Установка модуля Salt Minion на сервер Ankey SIEM NG Server²² (см. пункт 3.11.1).
 - 7.2 Установка роли RMQ Message Bus²³ (см. пункт 3.11.2).
 - 7.3 Установка роли SIEM Server (см. пункт 3.11.3).
8. Установка компонента Ankey SIEM NG Collector (см. подраздел 3.12):
 - 8.1 Установка модуля Salt Minion на сервер Ankey SIEM NG Collector²⁴ (см. пункт 3.15.1).
 - 8.2 Установка роли Collector (см. пункт 3.15.2).
9. Установка облегченной версии Ankey SIEM NG Server:
 - 9.1 Установка модуля Salt Minion (см. пункт 3.17.1).
 - 9.2 Установка роли RMQ Message Bus (см. пункт 3.17.2).
 - 9.3 Установка роли SIEM Server (см. пункт 3.17.3).
10. Активация лицензии (см. подраздел 3.12).
11. Установка стандартной базы данных (см. подраздел 3.14).
12. Установка и первоначальная настройка локального сервера обновлений Ankey Update Mirror (опционально) (см. подраздел 3.23.5).
13. Установка и первоначальная настройка компонента Ankey SIEM NG RC (опционально) (см. подраздел 3.20):
 - 12.1 Установка модуля Salt Minion (см. пункт 3.20.1).
 - 12.2 Установка роли RMQ Message Bus (см. пункт 3.20.2).
 - 12.3 Установка роли Retro Correlator (см. пункт 3.20.3).
14. Настройка Ankey SIEM NG для обеспечения его безопасной работы (см. подраздел 3.24).

²¹ В конфигурации для низконагруженных систем установка модуля Salt Minion на сервер Ankey SIEM NG Events Storage не требуется.

²² Данный шаг необходимо выполнить, если Ankey SIEM NG Core установлен на Linux в конфигурации для высоконагруженных систем. В конфигурации для средненагруженных систем модуль Salt Minion устанавливается на сервер Ankey SIEM NG Server при установке компонента Ankey SIEM NG Events Storage.

²³ Данный шаг необходимо выполнить, если Ankey SIEM NG Server устанавливается в конфигурации для средненагруженных, высоконагруженных систем.

²⁴ Данный шаг необходимо выполнить, если Ankey SIEM NG Collector устанавливается на отдельный сервер.

3.6 Установка роли Deployer

Для установки роли вам потребуется архив `Deployer_<Номер версии>.tar.gz` из комплекта поставки.

Роль необходимо устанавливать на сервер Ankey SIEM NG Core или на сервер Ankey SIEM NG Server.

Внимание! Для любой конфигурации Ankey SIEM NG необходимо установить только один экземпляр роли Deployer. Установка второго экземпляра роли Deployer на сервер любого компонента сделает работу Ankey SIEM NG невозможной и потребует переустановки всей системы.

Внимание! Для корректной работы Ankey SIEM NG необходимо, чтобы подсеть его Docker-контейнеров не совпадала с подсетями, используемыми в организации. По умолчанию система виртуализации Docker использует подсеть 172.17.0.0/12. Если эта подсеть уже используется вашим оборудованием, вы можете изменить подсеть во время развертывания Ankey SIEM NG при установке роли Deployer. Для этого в наборе конфигурационных параметров **Advanced configuration** необходимо указать в качестве значения параметра **CustomDockerAddressPool** подсеть, отличную от используемых в вашей организации, а в качестве значения параметра **CustomDockerNetworkSize** – размер этой подсети (рекомендуется использовать значение, не превышающее 25 бит). Вы также можете изменить подсеть Docker-контейнера уже установленного Ankey SIEM NG по инструкции из раздела «Подсеть Docker-контейнера Ankey SIEM NG совпадает с одной из подсетей предприятия» Руководства администратора Ankey SIEM NG.

Внимание! На сервере, на который необходимо установить роль Deployer, порты 4505/TCP, 4506/TCP, 5000/TCP должны быть доступны для входящих соединений.

Для установки роли вам потребуется архив `Deployer_<Номер версии>.tar.gz` из комплекта поставки.

Чтобы установить роль:

1. Если роль устанавливается на сервере с Astra Linux, отключите на этом сервере обязательный ввод пароля для выполнения команды `sudo`:
`sudo astra-sudo-control disable`
2. Если на сервере, на который устанавливается роль Deployer, есть файл `/etc/salt/pki/minion/minion_master.pub`, удалите его:
`rm /etc/salt/pki/minion/minion_master.pub`
3. Распакуйте архив `Deployer_<Номер версии>.tar.gz`:
`tar -xvf Deployer_<Номер версии>.tar.gz`
4. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
5. В открывшемся окне нажмите кнопку **Yes**.
Начнутся распаковка и подготовка пакетов. По завершении подготовки откроется окно с текстом лицензионного соглашения.

6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
Откроется окно для проверки и изменения параметров установки.
7. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.
8. Убедитесь, что в качестве значения параметра HostAddress указано полное доменное имя (FQDN) или IPv4-адрес сервера, на который устанавливается роль Deployer.

Внимание! Если в параметре HostAddress указать значение localhost, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

9. Нажмите кнопку **OK**.
Начнется установка пакетов. По завершении установки появится сообщение Deployment configuration successfully applied.
10. Нажмите кнопку **OK**.
11. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.
Роль установлена.

3.7 Установка компонента Ankey SIEM NG MC

Компонент Ankey SIEM NG Management and Configuration необходимо установить на одну операционную систему с компонентом Ankey SIEM NG Core.

Установка компонента Ankey SIEM NG Management and Configuration делится на следующие этапы:

1. Установка модуля Salt Minion – если роль Deployer установлена на сервер Ankey SIEM NG Server или отдельно.

Внимание! Если на сервере, на котором разворачивается компонент, уже установлена роль Deployer, установка модуля Salt Minion не требуется.

2. Установка роли SqlStorage/JatobaStorage.
3. Установка роли Management and Configuration.

Перед установкой компонента Ankey SIEM NG MC необходимо принять решение, какая именно роль будет установлена: SqlStorage (СУБД PostgreSQL) или JatobaStorage (СУБД Jatoba).

Для установки роли JatobaStorage потребуется:

- доступ к глобальной сети Интернет (для получения лицензии в режиме онлайн или офлайн);
- действующий ключ активации для СУБД Jatoba.

3.7.1 Установка модуля Salt Minion на сервер Ankey SIEM NG Core

Внимание! Для средненагруженных и высоконагруженных систем на сервере, на который устанавливается модуль Salt Minion, порт 22/TCP должен быть открыт для входящих соединений.

Чтобы установить модуль Salt Minion:

1. Если на сервере Ankey SIEM NG Core есть файл `/etc/salt/pki/minion/minion_master.pub`, удалите его:
`rm /etc/salt/pki/minion/minion_master.pub`
2. Если Ankey SIEM NG Core устанавливается на Astra Linux, на сервере Ankey SIEM NG Core отключите обязательный ввод пароля для выполнения команды `sudo`:
`sudo astra-sudo-control disable`
3. Если Ankey SIEM NG Core устанавливается на Debian, на сервере компонента установите утилиту `sudo`, выполнив в интерфейсе терминала команду от имени суперпользователя (root):
`apt-get install sudo`
4. Если Ankey SIEM NG Core устанавливается на Debian, на сервере компонента отключите обязательный ввод пароля для выполнения команды `sudo`, добавив в файл `/etc/sudoers` строку:
<Логин учетной записи, от имени которой устанавливается компонент>
`ALL=(ALL:ALL) NOPASSWD: ALL`
5. На сервере с установленной ролью Deployer запустите сценарий:
`/var/lib/deployer/role_packages/<название каталога, например Deployer_1_14_2868>/deploy_minion.sh`
6. В открывшемся окне введите IP-адрес или FQDN сервера Ankey SIEM NG Core и нажмите кнопку **ОК**.

Внимание! Если в параметре **HostAddress** указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать IP-адрес или FQDN сервера.

7. В открывшемся окне введите логин учетной записи, от имени которой устанавливается компонент, на сервере Ankey SIEM NG Core и нажмите кнопку **ОК**.
8. В окне **Info** нажмите кнопку **ОК**.
9. Введите пароль учетной записи с правами суперпользователя (root) на сервере Ankey SIEM NG Core.
10. Запустится установка модуля Salt Minion.
11. Если требуется, в открывшемся окне введите FQDN сервера и нажмите кнопку **ОК**.
12. По завершении установки появится сообщение `Minion on '<IP-адрес или FQDN сервера>' successfully installed.`

Модуль Salt Minion установлен.

3.7.2 Установка роли SqlStorage

Для установки роли вам потребуется архив `sqlstorage_<Номер версии>.tar.gz` из комплекта поставки.

Чтобы установить роль:

1. На сервере Ankey SIEM NG Core распакуйте архив `sqlstorage_<Номер версии>.tar.gz`:
`tar -xf sqlstorage_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения Management and Configuration и нажмите кнопку **OK**.
6. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.

Внимание! Можно создать только один экземпляр (Instance).

7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем или IPv4-адресом сервера Ankey SIEM NG Core.
9. В открывшемся окне введите название экземпляра роли SqlStorage и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
10. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.
11. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Core.

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

12. Нажмите кнопку **OK**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
 13. Нажмите кнопку **OK**.
- Роль установлена.

3.7.3 Установка роли JatobaStorage и онлайн активация лицензии

Для установки роли вам потребуется архив `jatobastorage_<Номер версии>.tar.gz` из комплекта поставки.

Чтобы установить роль:

1. На сервере Ankey SIEM NG Core распакуйте архив `jatobastorage_<Номер версии>.tar.gz`:
`tar -xvf jatobastorage_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения **Management and Configuration** и нажмите кнопку **OK**.
6. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.
7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем или IPv4-адресом сервера Ankey SIEM NG Core.
9. В открывшемся окне введите название экземпляра роли **JatobaStorage** и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
10. Для выполнения онлайн активации СУБД Jatoba следует выбрать вариант **Basic configuration**.
Откроется список основных параметров для настройки установки СУБД.
11. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) сервера Ankey SIEM NG Core или его IPv4-адрес.

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

12. В поле **JatobaLicenseActivationType** выберите значение `online`.
13. В поле **LicenceKey** удалите значение по умолчанию `XXXXX-XXXXX-XXXXX-XXX` и вручную введите ключ для активации СУБД Jatoba.
14. Если устанавливается роль **JatobaStorage** с лицензией, для которой необходимо подтверждение по электронной почте, в качестве значения параметра **LicenseEmail** укажите адрес электронной почты, указанный при получении лицензии.
15. В поле **LicenseServerUri** по умолчанию должно содержаться значение `https://licence.gaz-is.ru`.
16. Значения в других полях следует оставить по умолчанию.

17. Нажмите кнопку **ОК**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
18. Выберите **ОК** и нажмите на клавиатуре клавишу **Enter**.
Роль установлена.

Внимание! Перед установкой других ролей ПК Ankey SIEM NG необходимо проверить работоспособность docker-контейнера с СУБД Jatoba. После установки роли JatobaStorage выполнить команду `docker ps -a`.

В результате вывода команды должны содержаться данные обо всех установленных docker-контейнерах и их состоянии. Название docker-контейнера с СУБД Jatoba будет зависеть от названия роли (например: `storage-jatoba`). В колонке `STATUS` должно быть значение `UP` <количество времени>, в течение которого docker-контейнер с СУБД Jatoba активен. Docker-контейнер с СУБД Jatoba должен быть активен не менее, чем 3 минуты и не перезапускаться с интервалом до 30 секунд.

Чтобы проверить статус активации лицензии СУБД Jatoba в логах, следует выполнить команду `docker ps -a` и определить `CONTAINER ID` для docker-контейнера.

Для вывода логов docker-контейнера с СУБД Jatoba следует выполнить команду `docker logs <идентификатор docker-контейнера, например 20d228ccd15f>`. В логах docker-контейнера СУБД Jatoba не должно содержаться сообщений типа: `[license info]: license file name: /license/jatoba.cer (not found)`

3.7.4 Установка роли JatobaStorage и офлайн активация лицензии

Для установки роли вам потребуется архив `jatobastorage_<Номер версии>.tar.gz` из комплекта поставки.

Чтобы установить роль:

1. На сервере Ankey SIEM NG Core распакуйте архив `jatobastorage_<Номер версии>.tar.gz`:
`tar -xvf jatobastorage_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения **Management and Configuration** и нажмите кнопку **ОК**.
6. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.
7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем или IPv4-адресом сервера Ankey SIEM NG Core.

9. В открывшемся окне введите название экземпляра роли JatobaStorage и нажмите кнопку **ОК**.
Откроется окно для проверки и изменения параметров установки.
10. Для выполнения онлайн активации СУБД Jatoba следует выбрать вариант **Basic configuration**.
Откроется список основных параметров для настройки установки СУБД.
11. Убедитесь, что в качестве значения параметра HostAddress указано полное доменное имя (FQDN) сервера Ankey SIEM NG Core или его IPv4-адрес.

Внимание! Если в параметре HostAddress указать значение localhost, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

12. В поле **JatobaLicenseActivationType** выберите значение offline.
13. В поле **LicenceKey** удалите значение по умолчанию XXXXX-XXXXX-XXXXX-XXXX и вручную введите ключ для активации СУБД Jatoba.
14. Если устанавливается роль JatobaStorage с лицензией, для которой необходимо подтверждение по электронной почте, в качестве значения параметра **LicenseEmail** укажите адрес электронной почты, указанный при получении лицензии.
15. В поле **LicenseServerUri** по умолчанию должно содержаться значение <https://licence.gaz-is.ru>.
16. Значения в других полях следует оставить по умолчанию.
17. Нажмите кнопку **ОК**.
Начнется установка пакетов. По завершении установки появится сообщение Deployment configuration successfully applied.
18. Выберите **ОК** и нажмите на клавиатуре клавишу **Enter**.
Роль установлена.

Для офлайн активации лицензии:

1. После установки роли JatobaStorage перейдите в каталог /var/lib/deployed-roles/<Название приложения Ankey SIEM NG MC, например: mc-application-ankey>/<Название роли СУБД Jatoba, например: jatobastorage>/config/license/ и проверьте наличие файла request.dat.
2. Перенесите файл request.dat на хост с доступом к глобальной сети Интернет.
3. В веб-браузере хоста с доступом к глобальной сети интернет необходимо перейти на сайт <https://license.gaz-is.ru/offlineActivate/>. В веб-браузере должна отобразиться страница **Офлайн-активация**.
4. Для формирования запроса на офлайн активацию лицензии СУБД Jatoba скопируйте в окно ввода активационный запрос для получения файла лицензии или скопируйте и вставьте запрос из файла request.dat.

- В ответ на запрос из файла `request.dat` будет предоставлен файл лицензии `license.bin`.
5. Сохраните на хосте файл `license.bin` и переименуйте с соблюдением регистра в `jatoba.cer`.
 6. Скопируйте файл `jatoba.cer` в каталог `/var/lib/deploymodes/<название приложения> Management and Configuration`, например: `mc-application-ankey/<название роли СУБД> Jatoba`, например: `jatobastorage>/config/license/`.
 7. Лицензия для СУБД Jatoba активирована.

Примечание. Подробнее о получении лицензии с активацией офлайн вы можете прочитать в Руководстве по установке СУБД Jatoba на сайте производителя.

Внимание! Перед установкой других ролей ПК Ankey SIEM NG необходимо проверить работоспособность docker-контейнера с СУБД Jatoba. После установки роли JatobaStorage выполнить команду `docker ps -a`.

В результате вывода команды должны содержаться данные обо всех установленных docker-контейнерах и их состоянии. Название docker-контейнера с СУБД Jatoba будет зависеть от названия роли (например: `storage-jatoba`). В колонке STATUS должно быть значение UP <количество времени>, в течение которого docker-контейнер с СУБД Jatoba активен. Docker-контейнер с СУБД Jatoba должен быть активен не менее чем 3 минуты и не перезапускаться с интервалом до 30 секунд.

Чтобы проверить статус активации лицензии СУБД Jatoba в логах следует выполнить команду `docker ps -a` и определить CONTAINER ID для docker-контейнера.

Для вывода логов docker-контейнера с СУБД Jatoba следует выполнить команду `docker logs <идентификатор docker-контейнера>`, например `20d228ccd15f`. В логах docker-контейнера СУБД Jatoba не должно содержаться сообщений типа `[license info]: license file name: /license/request.dat (not found)`

3.7.5 Установка роли Management and Configuration

Внимание! Если вы устанавливаете Ankey SIEM NG с дополнительным компонентом VM²⁵ в изолированном сегменте сети без прямого подключения к интернету, для получения обновлений базы уязвимостей необходимо предварительно установить и настроить локальный сервер обновлений в соответствии с инструкциями в разделе «Настройка обновления экспертных данных» (см. раздел 3.22)

Для установки роли вам потребуется архив `managementandconfiguration_<Номер версии>.tar.gz` из комплекта поставки и токен аутентификации, который хранится в файле `instance-access-token.key` и представляет собой набор символов, закодированных с использованием стандарта Base64. Этот набор символов необходимо будет указать в качестве

²⁵ Центр обновлений экспертных данных Ankey SIEM NG доступен в исполнениях Ankey SIEM NG VM и Ankey SIEM NG с дополнительным компонентом VM

значения конфигурационного параметра `PackagesSourceCredentialToken` на одном из шагов инструкции.

Примечание. Новые пользователи Ankey SIEM NG получают файл **instance-access-token.key** вместе с лицензией на продукт, а существующие пользователи, обновляющиеся с версии 4.1 – вместе с дистрибутивом или через службу технической поддержки.

Чтобы установить роль:

1. На сервере Ankey SIEM NG Core распакуйте архив `managementandconfiguration_<Номер версии>.tar.gz`:
`tar -xf managementandconfiguration_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выберите вариант с идентификатором приложения **Management and Configuration**.
5. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.

Внимание! Можно создать только один экземпляр (Instance).

6. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG Core.
8. В открывшемся окне введите название экземпляра роли **Management and Configuration** и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
9. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.
10. В качестве значения параметра `DefaultLocale` выберите язык веб-интерфейса приложения **Management and Configuration**.
11. Убедитесь, что в качестве значения параметров `HostAddress` и `PostgreHost` указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Core.

Внимание! Если в параметрах указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

12. В качестве значения параметра `ExpertDataUpdateMethod` выберите:

для исполнения Ankey SIEM NG	для исполнения Ankey SIEM NG с дополнительным компонентом VM
Offline	– если обновление экспертных данных будет осуществляться напрямую с сервера обновлений «Газинформсервис» или с помощью локального сервера обновлений – Online.; – если вручную – Offline.

13. В качестве значения параметра `PackagesSourceUri` укажите:
- если вы устанавливаете Ankey SIEM NG в сегменте сети с прямым подключением к интернету – адрес глобального сервера обновлений
`https://update.ptsecurity.com/packman/v1/;`
 - если в изолированном сегменте сети без прямого подключения к интернету – адрес локального сервера обновлений в формате
`http://<Адрес сервера>:<Порт>/packman/v1/.`

Примечание. Указанный в параметре порт локального сервера обновлений должен быть открыт для входящих соединений. Для подключения по протоколам HTTP и HTTPS по умолчанию используются порты 8553 и 8743 соответственно.

В качестве значения параметра `PackagesSourceCredentialToken` укажите содержимое файла `instance-access-token.key`.

Примечание. Откройте файл `instance-access-token.key` с помощью любого текстового редактора. Скопируйте содержимое из файла `instance-access-token.key` и вставьте в поле `PackagesSourceCredentialToken` с помощью сочетания клавиш **Shift+Insert**.

- Нажмите кнопку **ОК**.
- Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied.`
- Нажмите кнопку **ОК**.
- Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль установлена.

3.8 Установка компонента Knowledge Base

Компонент Knowledge Base устанавливается с помощью роли Knowledge Base. Для установки роли вам потребуется архив `kb_<Номер версии>.tar.gz` из комплекта поставки.

Чтобы установить роль:

1. На сервере с установленной ролью Deployer распакуйте архив `kb_<Номер версии>.tar.gz`:
`tar -xf kb_<Номер версии>.tar.gz.`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения Knowledge Base и нажмите кнопку **OK**.
6. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.

Внимание! Можно создать только один экземпляр (Instance).

7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG Core.
9. В открывшемся окне введите название экземпляра роли Knowledge Base и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
10. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.
11. В качестве значения параметра **DefaultLocale** выберите желаемый язык интерфейса приложения Knowledge Base.

Внимание! Укажите значения параметров:

HostAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>

PostgreHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>

MCAddress: `https://<FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:3334`

CoreAddress: `https://<FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:443`

Внимание! Если в параметрах указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

12. Нажмите кнопку **OK**.

Начнется установка пакетов. По завершении установки появится сообщение **Deployment configuration successfully applied**.

13. Нажмите кнопку **OK**.
14. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль установлена.

3.9 Установка компонента Ankey SIEM NG Core

Компонент Ankey SIEM NG Core устанавливается с помощью ролей RMQ Message Bus и Core в следующем порядке: сначала устанавливается роль RMQ Message Bus, затем роль Core.

Внимание! Для установки компонента Ankey SIEM NG Core необходимо, чтобы TCP-порт 80 был свободен. Если этот порт занят каким-либо веб-сервером, выключите этот веб-сервер, удалите его или перенесите на другой порт.

3.9.1 Установка роли RMQ Message Bus на сервер Ankey SIEM NG Core

Для установки роли вам потребуется архив `rmqmessagebus_<Номер версии>.tar.gz` из комплекта поставки.

Чтобы установить роль:

1. На сервере с установленной ролью Deployer распакуйте архив `rmqmessagebus_<Номер версии>.tar.gz`:
`tar -xvf rmqmessagebus_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнутся распаковка и подготовка пакетов, необходимых для установки.
По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения Ankey SIEM NG и нажмите кнопку **OK**.
6. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.

Внимание! Можно создать только один экземпляр (Instance).

8. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG Core.
9. В открывшемся окне введите название экземпляра роли RMQ Message Bus и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.

10. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.
11. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Core.

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

12. Нажмите кнопку **ОК**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
13. Нажмите кнопку **ОК**.
14. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль установлена.

3.9.2 Установка роли Core

Для установки роли вам потребуется архив `core_<Номер версии>.tar.gz` из комплекта поставки.

Чтобы установить роль:

1. На сервере Ankey SIEM NG Core распакуйте архив `core_<Номер версии>.tar.gz`:
`tar -xvf core_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для установки.
По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
6. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.

Внимание! Можно создать только один экземпляр (Instance).

7. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG Core.
8. В открывшемся окне введите название экземпляра роли Core и нажмите кнопку **ОК**.
Откроется окно для проверки и изменения параметров установки.
9. Выберите вариант **Basic configuration**.

- Откроется страница со списком основных параметров.
10. В качестве значения параметра **DefaultLocale** выберите желаемый язык интерфейса приложения Ankey SIEM NG.

Внимание! Укажите корректные значения основных параметров:

HostAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>

MCAAddress: https://<FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:3334

KBAddress: https://<FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:8091

PostgreHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>

RMQHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>

SiemFrontendAddress: https://<FQDN или IPv4-адрес сервера Ankey SIEM NG Server>:8013>

Внимание! Если в параметрах указать значение localhost, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

11. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль установлена.

3.10 Установка компонента Ankey SIEM NG Events Storage

Компонент Ankey SIEM NG Events Storage устанавливается с помощью одной из ролей – с хранилищем событий Elasticsearch или с хранилищем событий LogSpace²⁶.

Внимание! Хранилище событий LogSpace имеет следующие ограничения функциональных возможностей:

- нет горячих и холодных индексов для хранения событий ИБ;
- нет поддержки работы ПК Ankey SIEM NG с несколькими конвейерами, связанными с одним ядром (компонентом Ankey SIEM NG Core);
- нет поддержки распределенного поиска событий ИБ между площадками, которые объединены в одну иерархию;
- нет функциональных возможностей для создания кластера из LogSpace.

Перед установкой роли необходимо установить модуль Salt Minion на

²⁶ Дистрибутив роли LogSpace является опциональным хранилищем ПК Ankey SIEM NG и предоставляется по запросу к производителю с учетом принятия действующих ограничений по функциональным возможностям. Полная функциональность доступна в хранилище событий Elasticsearch.

сервер Ankey SIEM NG Events Storage в конфигурациях для высоконагруженных систем и для конфигураций для средненагруженных систем. В конфигурации для низконагруженных систем установка модуля Salt Minion на сервер Ankey SIEM NG Events Storage не требуется.

Внимание! Если на сервере, на котором разворачивается компонент, уже установлена роль Deployer, установка модуля Salt Minion не требуется.

Для хранения событий доступны два типа хранилищ – Elasticsearch и LogSpace. Выбранное хранилище будет установлено при установке соответствующей роли.

Внимание! При разворачивании Ankey SIEM NG с несколькими конвейерами необходимо устанавливать роль SIEM Storage с хранилищем событий Elasticsearch.

3.10.1 Установка модуля Salt Minion на сервер Ankey SIEM NG Events Storage

Для установки Ankey SIEM NG Events Storage на Debian, на сервере компонента должна быть установлена утилита `sudo`. Вы можете установить ее с помощью команды `apt-get install sudo`. Команду необходимо вводить в интерфейсе терминала от имени суперпользователя (`root`).

Внимание! Для средненагруженных и высоконагруженных систем на сервере, на который устанавливается модуль Salt Minion, порт 22/TCP должен быть открыт для входящих соединений.

Чтобы установить модуль Salt Minion:

1. Если на сервере Ankey SIEM NG Events Storage есть файл `/etc/salt/pki/minion/minion_master.pub`, удалите его:
`rm /etc/salt/pki/minion/minion_master.pub`
2. Если Ankey SIEM NG Events Storage устанавливается на Astra Linux, на сервере компонента отключите обязательный ввод пароля для выполнения команды `sudo`:
`sudo astra-sudo-control disable`
3. Если Ankey SIEM NG Events Storage устанавливается на Debian, на сервере компонента установите утилиту `sudo`, выполнив в интерфейсе терминала команду от имени суперпользователя (`root`):
`apt-get install sudo`
4. Если Ankey SIEM NG Events Storage устанавливается на Debian, на сервере компонента отключите обязательный ввод пароля для выполнения команды `sudo`, добавив в файл `/etc/sudoers` строку:
<Логин учетной записи, от имени которой устанавливается компонент>
`ALL=(ALL:ALL) NOPASSWD: ALL`
5. На сервере с установленной ролью Deployer запустите сценарий:
`/var/lib/deployer/role_packages/Deployer_<Номер версии>/deploy_minion.sh`

6. В открывшемся окне введите полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Events Storage и нажмите кнопку **OK**.

Внимание! Если в окне указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

7. В открывшемся окне введите логин учетной записи, от имени которой устанавливается компонент, на сервере Ankey SIEM NG Events Storage и нажмите кнопку **OK**.
8. В открывшемся окне **Info** нажмите кнопку **OK**.
9. Введите пароль учетной записи с правами суперпользователя на сервере Ankey SIEM NG Events Storage. Запустится установка модуля Salt Minion.
10. Если требуется, в открывшемся окне введите FQDN или IPv4-адрес сервера и нажмите кнопку **OK**. По завершении установки появится сообщение `Minion on '<FQDN или IPv4-адрес сервера>' successfully installed`.

Модуль Salt Minion установлен.

3.10.2 Установка роли SIEM Storage с хранилищем событий Elasticsearch

Внимание! Не устанавливайте роль Event Storage на серверы с распределенными файловыми системами, например NFS.

Для установки роли вам потребуется архив `ankey_siemstorage_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере с установленной ролью Deployer распакуйте архив `ankey_siemstorage_<Номер версии>.tar.gz`:
`tar -xvf ankey_siemstorage_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**. Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выполните одно из следующих действий:
 - если в открывшемся окне для выбора доступен вариант с идентификатором установленного ранее приложения Ankey SIEM NG – выберите этот вариант;
 - если вариант с идентификатором установленного ранее приложения Ankey SIEM NG отсутствует – выберите вариант **Create New Application**.
5. Если вы выбрали вариант **Create New Application**, в открывшемся окне введите идентификатор приложения Ankey SIEM NG и нажмите кнопку **OK**.

6. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.

Внимание! Можно создать только один экземпляр (Instance).

7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG Events Storage.
9. В открывшемся окне введите название экземпляра роли SIEM Storage и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
10. Выберите набор параметров:
 - если ПК Ankey SIEM NG разворачивается в конфигурации для низконагруженных или средненагруженных систем, выберите вариант **Basic configuration**²⁷;
 - если ПК Ankey SIEM NG разворачивается в конфигурации для высоконагруженных систем, выберите вариант **Advanced configuration**.

Откроется страница с перечнем параметров конфигурации.

11. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Events Storage.

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

12. Если требуется установить Ankey SIEM NG Events Storage на сервер с публичным IP-адресом, присвойте параметру **ElasticsearchGlobalAccess** значение `True`.

Параметр **ElasticsearchGlobalAccess** доступен только в наборе параметров **Advanced configuration**.

Внимание! Использование сервера с публичным IP-адресом для Ankey SIEM NG Events Storage требует осторожности: если незащищенный сервер будет подключен к интернету, любой человек сможет скачать, изменить или удалить ваши данные.

13. Укажите значение параметра **ClusterConfigurationProfile**:
 - если ПК Ankey SIEM NG разворачивается в конфигурации для низконагруженных систем, выберите вариант **AIO**;
 - если для средненагруженных систем – вариант **SIEMandStorage**;

²⁷ Можно выбрать **Advanced configuration** для разворачивания средненагруженных систем, потому что данный вариант предоставляет возможность гибкой настройки под любые условия.

- если для высоконагруженных систем с потоком событий до 20000 в секунду – **Standalone**²⁸;
 - если для высоконагруженных систем с потоком событий выше 20000 в секунду – **ManagedStorage**;
 - если необходимо изменить объем оперативной памяти, выделяемый узлам кластера Elasticsearch, выберите вариант **Manual**.
14. Если в качестве значения параметра **ClusterConfigurationProfile** выбран вариант **Manual**, введите в качестве значений параметров **MasterNodeHeapSize**, **ClientNodeHeapSize** и **DataNodeHeapSize** объем оперативной памяти, выделяемый для главного узла, клиентского узла и узла данных соответственно.

Примечание. Минимальное значение параметров **MasterNodeHeapSize** и **ClientNodeHeapSize** – 2 ГБ, параметра **DataNodeHeapSize** – 8 ГБ. Суммарный объем оперативной памяти всех узлов кластера, умноженный на коэффициент 1.5, не должен превышать объем оперативной памяти сервера Ankey SIEM NG Events Storage.

15. Если ПК Ankey SIEM NG разворачивается в конфигурации для высоконагруженных систем и сервер Ankey SIEM NG Events Storage имеет емкость ОЗУ 256 ГБ или более, установите флажок **HighLoad**.

Примечание. В случае установки флажка **HighLoad** кластер Elasticsearch будет содержать четыре узла данных.

16. Если требуется, измените значения параметров в автоматически созданных каталогах:
- PathData: <Каталог для хранения индексов>

Примечание. В высоконагруженных системах каталог используется для хранения индексов, находящихся в теплой стадии, а также для хранения счетчиков всех индексов.

- PathDataHot: <Каталог для хранения индексов, находящихся в горячей стадии>

Примечание. Каталог используется только для для высоконагруженных систем.

- PathRepo: <Каталог для хранения резервных копий индексов>
- PathLog: <Каталог для хранения файлов журналов>

²⁸ Для более детальной настройки ресурсов можно выбирать **Manual**.

Примечание. Подробное описание жизненного цикла индексов приведено на сайте elastic.co.

17. Нажмите кнопку **ОК**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
18. Нажмите кнопку **ОК**.
19. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль установлена.

3.10.3 Установка роли SIEM Storage с хранилищем событий LogSpace

Внимание! Не устанавливайте роль Event Storage на серверы с распределенными файловыми системами, например NFS.

Внимание! Для установки или обновления роли Event Storage с хранилищем событий LogSpace на Debian необходима ОС на базе ядра Linux версии 5.10. Подробные инструкции по обновлению ядра можно найти на сайте производителя.

Для установки роли вам потребуется архив `ankey_eventstorage_<Номер версии>.tar.gz` из комплекта поставки.

Чтобы установить роль:

1. На сервере с установленной ролью Deployer распакуйте архив `ankey_eventstorage_<Номер версии>.tar.gz`:
`tar -xf ankey_eventstorage_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выполните одно из следующих действий:
 - если в открывшемся окне для выбора доступен вариант с идентификатором установленного ранее приложения Ankey SIEM NG – выберите этот вариант;
 - если вариант с идентификатором установленного ранее приложения Ankey SIEM NG отсутствует – выберите вариант **Create New Application**.
5. Если вы выбрали вариант **Create New Application**, в открывшемся окне введите идентификатор приложения Ankey SIEM NG и нажмите кнопку **ОК**.
6. В окне **Instance selection** выберите вариант **Deploy New Instance**.
7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.

8. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG Events Storage.
9. В открывшемся окне введите название экземпляра роли Events Storage и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
10. Выберите вариант **Basic configuration**.
Откроется страница с перечнем параметров конфигурации.
11. В качестве значения параметра `PathData` укажите каталог для установки хранилища событий LogSpace.

Примечание. Для хранилища событий LogSpace рекомендуется использовать каталог `/data`.

12. Нажмите кнопку **OK**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
 13. Нажмите кнопку **OK**.
 14. На сервере с установленным хранилищем событий LogSpace откройте TCP-порты 8123 и 9000 для входящих соединений.
- Роль установлена.

3.11 Установка компонента Ankey SIEM NG Server

Установка компонента Ankey SIEM NG Server делится на следующие этапы:

1. Если Ankey SIEM NG Server устанавливается в конфигурации для высоконагруженных систем, то требуется установка модуля Salt Minion.

Примечание. В конфигурации для средненагруженных систем модуль Salt Minion устанавливается (см. пункт 3.11.1) на сервер Ankey SIEM NG Server при установке компонента Ankey SIEM NG Events Storage.

2. Если Ankey SIEM NG Server устанавливается в конфигурации для средненагруженных и высоконагруженных систем, то требуется установка роли RMQ Message Bus.
3. Если выполняется установка Ankey SIEM NG Server в конфигурации для низконагруженных систем, то устанавливается только роль SIEM Server. Второй экземпляр роли RMQ Message Bus не требуется устанавливать.

Внимание! Для средненагруженных и высоконагруженных систем модуль Salt Minion и компонент Ankey SIEM NG Server необходимо установить с сервера, где установлена роль Deployer.

3.11.1 Установка модуля Salt Minion на сервер Ankey SIEM NG Server

Внимание! Для средненагруженных и высоконагруженных систем на сервере, на который устанавливается модуль Salt Minion, порт 22/TCP должен быть открыт для входящих соединений.

Чтобы установить модуль Salt Minion:

1. Если на сервере Ankey SIEM NG Server есть файл `/etc/salt/pki/minion/minion_master.pub`, удалите его:
`rm /etc/salt/pki/minion/minion_master.pub`
2. Если Ankey SIEM NG Server устанавливается на Astra Linux, на сервере Ankey SIEM NG Server отключите обязательный ввод пароля для выполнения команды `sudo`:
`sudo astra-sudo-control disable`
3. Если Ankey SIEM NG Server устанавливается на Debian, на сервере компонента установите утилиту `sudo`, выполнив в интерфейсе терминала команду от имени суперпользователя (`root`):
`apt-get install sudo`
4. Если Ankey SIEM NG Server устанавливается на Debian, на сервере компонента отключите обязательный ввод пароля для выполнения команды `sudo`, добавив в файл `/etc/sudoers` строку:
<Логин учетной записи, от имени которой устанавливается компонент>
`ALL=(ALL:ALL) NOPASSWD: ALL`
5. На сервере с установленной ролью `deployer` запустите сценарий установки:
`/var/lib/deployer/role_packages/Deployer_<Номер версии>/deploy_minion.sh`
6. В открывшемся окне введите полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Server и нажмите кнопку **ОК**.

Внимание! Если в окне указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

7. В открывшемся окне введите логин учетной записи, от имени которой устанавливается компонент, на сервере Ankey SIEM NG Server и нажмите кнопку **ОК**.
8. В открывшемся окне **Info** нажмите кнопку **ОК**.
9. Введите пароль учетной записи с правами суперпользователя на сервере Ankey SIEM NG Server.
Запустится установка модуля Salt Minion.
10. Если требуется, в открывшемся окне введите FQDN или IPv4-адрес сервера и нажмите кнопку **ОК**.
По завершении установки появится сообщение `Minion on '<FQDN или IPv4-адрес сервера>' successfully installed.`

Модуль Salt Minion установлен.

3.11.2 Установка роли RMQ Message Bus на сервер Ankey SIEM NG Server

Для установки роли вам потребуется архив `rmqmessagebus_<Номер версии>.tar.gz` из комплекта поставки.

Чтобы установить роль:

1. На сервере с установленной ролью **Deployer** распакуйте архив `rmqmessagebus_<Номер версии>.tar.gz`:
`tar -xvf rmqmessagebus_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выберите вариант с идентификатором приложения **Ankey SIEM NG**.
5. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.

Внимание! Можно создать только один экземпляр (Instance).

6. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. В открывшемся окне выберите вариант с FQDN или IPv4-адрес сервера **Ankey SIEM NG Server**.
8. В открывшемся окне введите название экземпляра роли **RMQ Message Bus** и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
9. В наборе параметров выберите **Basic configuration**.
10. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) или IPv4-адрес сервера **Ankey SIEM NG Server**.

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

11. Нажмите кнопку **OK**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
12. Нажмите кнопку **OK**.
13. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль установлена.

3.11.3 Установка роли SIEM Server

Для установки роли вам потребуется архив `siemserver-linux_<Номер версии>.tar.gz` из комплекта поставки.

Чтобы установить роль:

1. На сервере с установленной ролью **Deployer** распакуйте архив `siemserver-linux_<Номер версии>.tar.gz`:
`tar -xf siemserver-linux_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выберите вариант с идентификатором приложения **Ankey SIEM NG**.
5. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.

Внимание! Можно создать только один экземпляр (Instance).

6. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. В открывшемся окне выберите вариант с доменным именем сервера **Ankey SIEM NG Server**.
8. В открывшемся окне введите название экземпляра роли **SIEM Server** и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
9. Выберите набор параметров:
 - если ПК Ankey SIEM NG разворачивается в конфигурации для низконагруженных или средненагруженных систем, выберите вариант **Basic configuration**;
 - если ПК Ankey SIEM NG разворачивается в конфигурации для высоконагруженных систем, выберите вариант **Advanced configuration**.

Откроется страница со списком параметров (см. приложение Б).

Внимание! Укажите значения параметров:

CoreAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>
HostAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Server>
RMQHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>

Внимание! Если в параметрах указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

10. Укажите значение параметра **StorageBackendType**:
 - если для хранения событий используется **Elasticsearch**, выберите вариант **elasticsearch**;

- если используется LogSpace – выберите вариант **logspace**.
- 11. Если ПК Ankey SIEM NG разворачивается в конфигурации для высоконагруженных систем, укажите полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Events Storage:
 - если для хранения событий используется Elasticsearch, измените значение параметра ElasticsearchHost:
ElasticsearchHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Events Storage выбранного конвейера>;
 - если для хранения событий используется LogSpace, измените значение параметра LogSpaceHost:
LogSpaceHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Events Storage выбранного конвейера>.

Внимание! При установке второго и последующих конвейеров в параметрах ElasticsearchHost и LogSpaceHost необходимо вручную указать IP-адрес или FQDN сервера Ankey SIEM NG Events Storage именно того конвейера, который вы устанавливаете.

- 12. Если ПК Ankey SIEM NG разворачивается в конфигурации для высоконагруженных систем с потоком событий выше 20000 событий в секунду, установите флажок **ManagedStorage**.
- 13. Если Ankey SIEM NG разворачивается в конфигурации для высоконагруженных систем и сервер Ankey SIEM NG Events Storage имеет емкость ОЗУ 256 ГБ или более, установите флажок **HighLoad**.

Примечание. В случае установки флажка **HighLoad** для службы SIEM server storage будет выделено шесть потоков операционной системы (вместо четырех, когда флажок снят).

- 14. Нажмите кнопку **ОК**.
Начнется установка пакетов. По завершении установки появится сообщение Deployment configuration successfully applied.
 - 15. Нажмите кнопку **ОК**.
 - 16. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.
- Роль установлена.

3.12 Активация лицензии ПК Ankey SIEM NG

Для активации лицензии вам потребуются следующие файлы из комплекта поставки:

- шаблон ключа <Номер лицензии>.grdvd;
- текстовый файл с серийным номером Ankey SIEM NG <Идентификатор ключа>.txt;
- мастер активации лицензий GuardantActivationWizard.exe (предназначен для офлайн-активации через ОС Microsoft Windows).

Активация лицензии выполняется на сервере компонента Ankey SIEM NG Core.

Если активировать несколько лицензий, система будет использовать только одну из них – имеющую самую раннюю дату окончания. Поэтому в случае приобретения продукта, который может быть развернут на базе уже установленного Ankey SIEM NG (например, приобретения дополнительного компонента VM) необходимо активировать объединенную лицензию на оба продукта (ее можно запросить в службе технической поддержки «Газинфорсервис»). В противном случае после активации отдельной лицензии на второй продукт в системе будет доступен набор функций только одного продукта.

После изменения аппаратной конфигурации сервера Ankey SIEM NG Core (например, по причине замены центрального процессора) необходимо повторно активировать лицензию. Количество таких повторных активаций ограничено – не более пяти раз. Дальнейшие попытки активации приведут к ошибке мастера активации «Количество активаций для введенного серийного номера исчерпано». Для получения нового шаблона ключа и нового серийного номера необходимо обратиться в службу технической поддержки (см. раздел 6).

Если вы повторно активировали лицензию (например, после переустановки ОС или компонента Ankey SIEM NG Core) и при этом не изменяли аппаратную конфигурацию сервера, счетчик активаций не уменьшается (количество таких повторных активаций не ограничено).

Информация о лицензии доступна на странице **Система → Управление системой**.

3.12.1 Активация лицензии на Linux при наличии доступа к интернету

Чтобы активировать лицензию:

1. На сервер Ankey SIEM NG Core в каталог /var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли Core>/data/licensing скопируйте шаблон ключа <Номер лицензии>.grdvd и текстовый файл с серийным номером <Идентификатор ключа>.txt.
2. Запустите активацию лицензии от имени суперпользователя (root):

```
docker exec -it $(docker ps | awk '/licensing/ {print $NF}')  
/usr/local/bin/guardantutils/grdspactivation /var/lib/microservice/<Номер  
лицензии>.grdvd /serialfile=/var/lib/microservice/<Идентификатор  
ключа>.txt
```

По завершении активации появится сообщение License activation Succeeded.

Лицензия активирована.

После активации лицензии необходимо перезапустить службы компонентов Ankey SIEM NG Core и Knowledge Base с помощью команды `docker restart $(docker ps -q -a)`, а затем выйти из системы и заново войти.

Кроме того, если ПК Ankey SIEM NG развертывается в средненагруженной или высоконагруженной конфигурации, после активации лицензии на сервере Ankey SIEM NG Server необходимо перезапустить следующие службы:

- Core Events Aggregator с помощью команды `docker restart $(docker ps | awk '/core-events-aggregator/ {print $NF}')`;
- Core Assets Premierger с помощью команды `docker restart $(docker ps | awk '/core-assets-premerger/ {print $NF}')`.

3.12.2 Активация лицензии на Linux при отсутствии доступа к интернету

Для активации лицензии вам потребуется рабочая станция с доступом в интернет и файл `GuardantActivationWizard.exe` из комплекта поставки.

Чтобы активировать лицензию:

1. На сервер Ankey SIEM NG Core в каталог `/var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли Core>/data/licensing` скопируйте шаблон ключа `<Номер лицензии>.grdvd` и текстовый файл с серийным номером `<Идентификатор ключа>.txt`.
2. Выполните команду от имени суперпользователя (root):
`docker exec -it $(docker ps | awk '/licensing/ {print $NF}') /usr/local/bin/guardantutils/grdspactivation /var/lib/microservice/<Номер лицензии>.grdvd /serialfile=/var/lib/microservice/<Идентификатор ключа>.txt /offline`
Мастер активации лицензий создаст в каталоге `/var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли Core>/data/licensing` файл `<Номер лицензии>.grdvd.toserver`.
3. На рабочей станции с доступом в интернет разместите в одной папке файлы `GuardantActivationWizard.exe` и `<Номер лицензии>.grdvd.toserver`.
4. Запустите файл `GuardantActivationWizard.exe`.
Откроется окно мастера активации лицензий.
5. Нажмите кнопку **Указать файл лицензии**.
6. В открывшемся окне выберите файл `<Номер лицензии>.grdvd.toserver` и нажмите кнопку **Открыть**.
7. Нажмите кнопку **Далее**.
Мастер активации лицензий создаст файл `<Номер лицензии>.grdvd.fromserver`. Папка с файлом откроется автоматически.
8. Нажмите кнопку **Готово**.

9. Скопируйте файл <Номер лицензии>.grdvd.fromserver на сервер Ankey SIEM NG Core в каталог /var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли Core>/data/licensing.
10. Выполните команду:

```
docker exec -it $(docker ps | awk '/licensing/ {print $NF}')
/usr/local/bin/guardantutils/grdspactivation /var/lib/microservice/<Номер
лицензии>.grdvd.fromserver
```

По завершении активации появится сообщение License activation Succeeded.

Лицензия активирована.

После активации лицензии необходимо перезапустить службы компонентов Ankey SIEM NG Core и Knowledge Base с помощью команды `docker restart $(docker ps -q -a)`, а затем выйти из системы и заново войти.

Кроме того, если ПК Ankey SIEM NG разворачивается в средненагруженной или высоконагруженной конфигурации, после активации лицензии на сервере Ankey SIEM NG Server необходимо перезапустить следующие службы:

- Core Events Aggregator с помощью команды `docker restart $(docker ps | awk '/core-events-aggregator/ {print $NF}')`;
- Core Assets Premerger с помощью команды `docker restart $(docker ps | awk '/core-assets-premerger/ {print $NF}')`.

3.13 Удаление лицензионного ключа

Чтобы удалить ключ на Linux, выполните команду:

```
docker exec -it $(docker ps | awk '/licensing/ {print $NF}')
/usr/local/bin/guardantutils/grdspactivation /delete=<Идентификатор ключа>
```

Ключ удален.

3.14 Установка стандартной базы данных, стандартных модулей сбора и обработки

Для работы с ресурсами в веб-интерфейсе ПК Ankey SIEM NG 5.2.3 необходимо:

1. Создать корневую базу данных **GIS_DB** (см. подраздел 3.14.1).
2. Установить в корневую базу данных пакет с актуальной таксономией **Taxonomy_5.x.kb** (см. подраздел 3.14.2).
3. Установить в корневую базу данных пакет стандартных коннекторов, который содержится в архиве **GIS_KB_ConnectorsStd_A.B.C.kb** (см. подраздел 3.14.3).
4. Извлечь из архива **GIS_KB_ContentStd_A.B.C.zip** файл **GIS_KB_ContentStd_A.B.C.kb**.
5. Установить в корневую базу данных пакет стандартного контента, который содержится в архиве **GIS_KB_ContentStd_A.B.C.kb** (см. подраздел 3.14.4).

Внимание! Необходимо сначала установить пакет стандартных коннекторов, а после пакет стандартного контента. Установка пакетов по отдельности или в другом порядке не рекомендуется, т.к. пакет стандартных коннекторов является основой для работы стандартного пакета контента.

Примечание. Создание и удаление корневой базы данных в Knowledge Base выполняется с помощью утилиты **kbtools**, которая устанавливается вместе с ролью Knowledge Base.

6. Создать ветку **Customer_Data** в корневой базе данных **GIS_DB**. Дождаться завершения процесса создания ветки **Customer_Data** (см. подраздел 3.14.5).
7. Установить программные инструменты разработки контента (SDK) (см. подраздел 3.14.6).
8. Установить ресурсы в Ankey SIEM NG (см. подраздел 3.14.7).

3.14.1 Создание корневой базы данных GIS_DB

Для создания корневой базы данных **GIS_DB** следует запустить от имени администратора интерфейс командной строки операционной системы Linux и выполнить команду:

```
/var/lib/deployed-roles/<Название приложения Knowledge Base>/<Название экземпляра роли приложения Knowledge Base, например kb-83dsp6udksxc1mdooulng>/tools/kbtools/kbtools createRootdb --db GIS_DB --db_name "GIS_DB" --kbHost <FQDN или IPv4 адрес сервера с компонентом Core> --iamHost <FQDN или IPv4-адрес сервера с компонентом Core> --login <Логин учетной записи с правами администратора> --password <Пароль от учетной записи с правами администратора>
```

Корневая база данных **GIS_DB** предназначена для хранения коннекторов и контента в исходном состоянии. Контент в базе данных следует устанавливать/обновлять²⁹ в полуавтоматическом режиме, используя функционал веб-интерфейса управления ПК Ankey SIEM NG.

3.14.2 Установка актуальной таксономии

Для того чтобы была возможность импортировать контент в базы данных ПК с помощью функционала веб-интерфейса необходимо установить корректную таксономию полей с помощью утилиты **kbtools**. Функционал веб-интерфейса не позволяет импортировать схему полей событий. После импорта схемы полей событий в новую базу данных возможно использовать функционал веб-интерфейса для импорта пакетов коннекторов и контента.

Для импорта пакета с актуальной таксономией **Taxonomy_5.2.kb** в корневую базу данных **GIS_DB** нужно запустить интерфейс командной строки операционной системы Linux, переключиться на учетную запись

²⁹ Алгоритм обновления ресурсов в базах данных представлен в документе «Руководство администратора Ankey SIEM NG 5.2.3».

суперпользователя (root) и выполнить команду:

```
/var/lib/deployed-roles/<Название приложения Knowledge Base>/<название экземпляра роли приложения Knowledge Base, например, <kb-83dspx6udksxc1mdooulng>/tools/kbtools/kbtools importPackage --db GIS_DB --kbHost <FQDN или IPv4 сервера с компонентом Core> --iamHost <FQDN или IPv4-адрес сервера с компонентом Core> --login <Логин учетной записи с правами администратора> --password <Пароль от учетной записи с правами администратора> --source "/opt/<название пакета><версия пакета с таксономией>.kb" --mode Upsert --ImportTaxonomy
```

3.14.3 Импорт пакета стандартных коннекторов и контента

❖ Для импорта пакета стандартных коннекторов **GIS_KB_Connectors_Std_A.B.C.kb**:

1. В веб-интерфейсе Ankey SIEM NG откройте выпадающий список компонентов, нажав на графический элемент .
2. В раскрывшемся меню выберите пункт **Knowledge Base**. Откроется веб-страница **Knowledge Base**.
3. В главном меню в разделе **<Название БД>** выберите пункт **Базы данных**. Откроется страница **Базы данных / <Название БД>**.



Рисунок 3.14 – Пункт Выпадающего меню Базы данных

4. В панели **Базы данных** выберите корневую базу данных **GIS_DB**.
5. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
Откроется страница **Пакеты экспертизы**;
6. В верхнем правом углу вкладки **Пакеты экспертизы** на панели инструментов выберите  **Импорт**.
7. В открывшемся диалоговом окне нажмите ссылку **выберите**, где будет предложено указать файл для загрузки, или переместите с помощью мыши файл пакета стандартных коннекторов **GIS_KB_Connectors_Std_A.B.C.kb** в специальное окно. После этого появится окно **Импорт объектов**.
8. Выполните импорт с параметрами, указанными на рисунке 3.15.

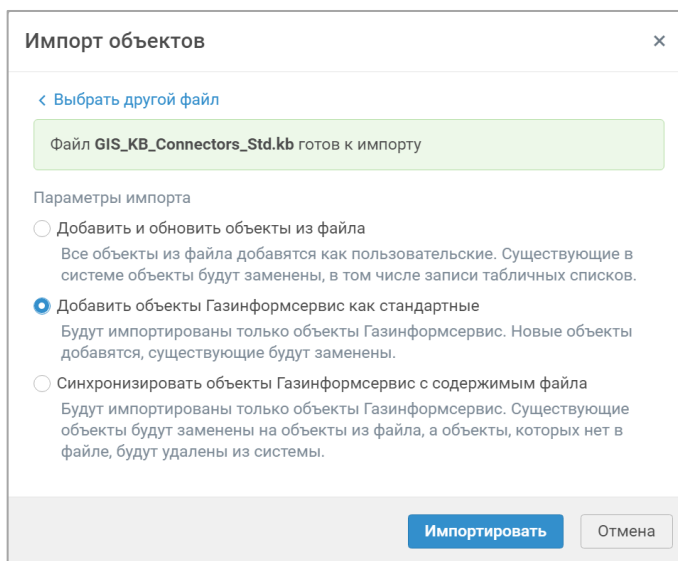


Рисунок 3.15 – Пример настройки параметров импорта коннекторов без возможности редактирования

После импорта пакета стандартных коннекторов в базу данных **GIS_DB** они будут недоступны для редактирования.

Установка пакетов дополнительных коннекторов описана в Приложении Д.1 «Установка дополнительных модулей сбора и обработки данных».

Внимание! После установки пакета стандартных коннекторов необходимо убедиться, что технологическое правило `DEV_Ankey_SIEM_NG_TTL` установилось в систему вместе с пакетом стандартных коннекторов. Если это правило не будет установлено, генератор событий TTL не будет работать.

3.14.4 Импорт пакета стандартного контента

❖ Для импорта пакета стандартного контента **GIS_KB_ContentStd_A.B.C.kb**:

1. В веб-интерфейсе Ankey SIEM NG откройте выпадающий список компонентов, нажав на графический элемент .
2. В раскрывшемся меню выберите пункт **Knowledge Base**. Откроется веб-страница **Knowledge Base**.
3. В главном меню в разделе **<Название БД>** выберите пункт **Базы данных**. Откроется страница **Базы данных / <Название БД>**.



Рисунок 3.16 – Пункт Выпадающего меню Базы данных

4. В панели **Базы данных** выберите корневую базу данных **GIS_DB**.

5. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
Откроется страница **Пакеты экспертизы**;
6. В верхнем правом углу вкладки **Пакеты экспертизы** на панели инструментов выберите  **Импорт**.
7. В открывшемся диалоговом окне нажмите ссылку **выберите**, где будет предложено указать файл для загрузки, или перетащите файл пакета стандартного контента **GIS_KB_ContentStd_A.B.C.kb** в диалоговое окно. После этого появится окно **Импорт объектов**.
8. Выполните импорт с параметрами, указанными на рисунке 3.17.

После импорта пакета стандартного контента в базу данных **GIS_DB** он будет недоступен для редактирования.

Установка пакетов дополнительного контента описана в Приложении Д.2 «Установка дополнительных модулей выявления нарушений ИБ (корреляционной обработки данных)».

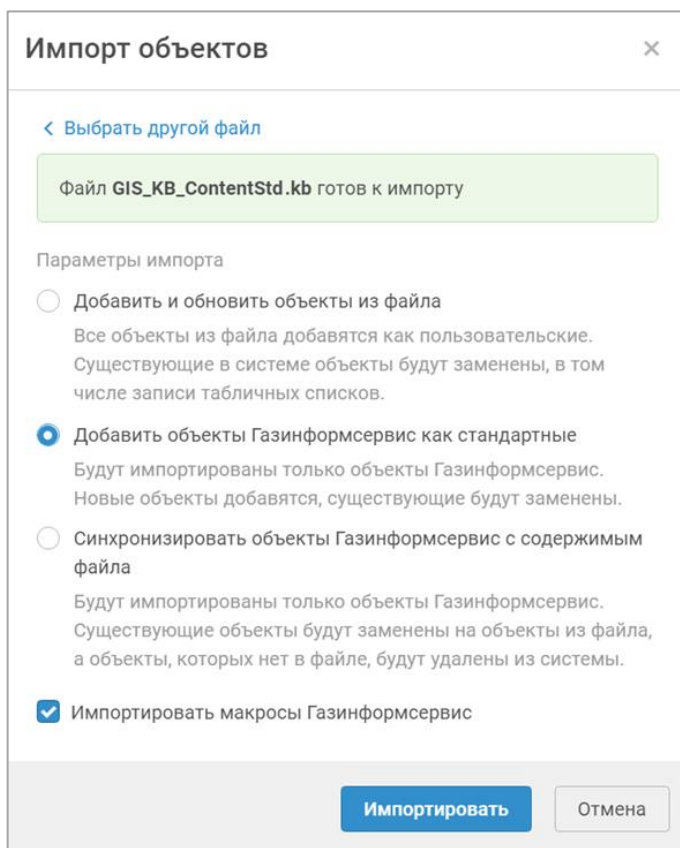


Рисунок 3.17 – Пример настройки параметров импорта контента без возможности редактирования и с добавлением макросов

3.14.5 Создание ветки Customer Data

❖ Чтобы создать ветку **Customer_Data** от корневой базы данных **GIS_DB**:

1. В приложении **Knowledge Base** в главном меню в разделе **<Название БД>** выберите пункт **Базы данных**.
Откроется страница **Базы данных / <Название БД>**.



Рисунок 3.18 – Пункт Выпадающего меню Базы данных

2. В панели **Базы данных** выберите корневую базу данных **GIS_DB**, созданную в разделе 3.14.1.

Внимание! Перед созданием ветки проверьте, что все необходимые наборы ресурсов (см. пункты 3.14.2 и 3.14.3) загружены в корневую базу данных.

3. в панели инструментов нажмите кнопку **+ Создать ветку**.
4. В открывшемся окне **Создание ветки** в поле **Имя** введите название **Customer_Data**.
5. В поле **Идентификатор** введите **Customer_Data**.
6. В блоке параметров **Модификаторы доступа** настройте параметры, как показано на рисунке 3.19:
 - Отметить:
 - **разрешить просмотр контента** – разрешение для пользователей на просмотр объектов в БД.
 - **разрешить редактирование контента** – разрешение на изменение объектов в БД;
 - Снять отметку:
 - **разрешить редактирование параметров базы данных** – разрешение на изменение параметров БД;
 - **разрешить слияние в базу данных** – разрешение на импорт объектов из родительской БД.

Рисунок 3.19 – Настройка параметров в блоке **Модификаторы доступа**

7. Нажмите кнопку **Сохранить**.
Начнется процесс создания ветки корневой базы данных.

Примечание. Процесс создания ветки занимает некоторое время в связи с копированием в нее ресурсов из родительской корневой базы данных.

8. После завершения создания ветка будет доступна для выбора;
В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
9. Откроется страница **Пакеты экспертизы**, где будет видно, что набор ресурсов в ветке установочной базы данных полностью идентичен набору ресурсов в корневой базе данных **GIS_DB**.

Внимание! Ресурсы сохранили свои свойства и являются стандартными, т.е. недоступными к изменению. Работа с ресурсами, установленными в Knowledge Base, описана в документе «Руководство оператора Ankey SIEM NG 5.2.3», раздел «Работа с Knowledge Base».

10. Выберите ветку **Customer_Data** в качестве установочной.
Для этого следует:
 - в приложении **Knowledge Base** в главном меню в разделе **<Название БД>** выбрать пункт **Базы данных**, нажав на графический элемент ;
 - выбрать пункт **Базы данных**. В качестве текущей базы данных выбрать ветку **Customer_Data** и нажать на  **Сделать установочной**.

Внимание! Базу данных GIS_DB нельзя использовать в качестве установочной, т.к. не гарантируются правильные дальнейшие обновления, а также сохранение пользовательских ресурсов.

3.14.6 Установка SDK

Перед валидацией и установкой контента необходимо выполнить установку программных инструментов разработки контента (SDK) для валидации контента (SDK). Для этого следует:

1. В приложении Knowledge Base открыть выпадающий список **SIEM** и выбрать **Выбор версии SDK**.
2. Выбрать версию SDK, например, 27.x.xxxx, а затем нажать на **Установить SDK для валидации**.

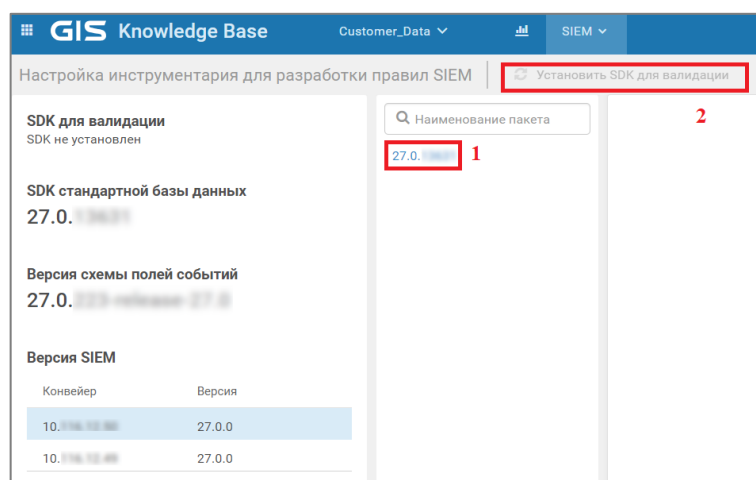


Рисунок 3.20 – Установка SDK

3. Открыть выпадающий список **SIEM** и выбрать **Пакеты экспертизы**.
4. Выделить в блоке правил в правой части веб-интерфейса весь контент с помощью сочетания клавиш **Ctrl+A** и выполнить валидацию, нажав на графическую кнопку . Валидация должна завершиться без ошибок.

3.14.7 Установка ресурсов в Ankey SIEM NG Server

❖ Чтобы корректно установить все необходимые ресурсы в компонент Server, нужно:

1. В главном меню в разделе **<Название базы данных>** выбрать ветку **Customer_Data**, созданную в разделе 3.14.5.

Внимание! Ветка **Customer_Data** является установочной БД, ресурсы, расположенные в родительской **GIS_DB**, доступны только для валидации и не устанавливаются в компонент Server.

2. В главном меню в разделе **SIEM** выбрать **Пакеты экспертизы**. Откроется страница **Пакеты экспертизы**.
3. Если набор для установки создавался ранее, перейти к п. 10.

Если набор для установки не требуется, то нужно выбрать набор «Все объекты» и перейти к п.17.

4. В панели **Наборы для установки** внизу слева нажать **+**. Откроется окно **Создание набора для установки**³⁰ (рисунок 3.21).

Рисунок 3.21 – Создание набора для установки

5. В поле **Системное название** ввести название набора. Рекомендуется указать системное название на латинице.
6. В поле **Название (русский)** возможно внести любое значение, оно будет отображаться в веб-интерфейсе. Например, «Основной набор для установки ресурсов».
7. В поле **Входит в набор** выбрать **Все объекты** или любой другой корректно сформированный набор для установки.
8. В поле **Устанавливать в конвейер** выбрать один или несколько конвейеров, в который будут установлены ресурсы из набора установки. Выбрать конвейеры для установки возможно только в том случае, если корректно выполнена установка всех основных компонентов ПК Ankey SIEM NG.

Внимание! На главном конвейере³¹ должны быть установлены все правила, которые есть на дополнительных конвейерах. Несоблюдение этого требования вызовет некорректную работу правил локализации. В случае установки коннектора не на главном конвейере, а только на целевом, необходимо продублировать пакеты ресурсов в главный конвейер.

³⁰ Подробно о наборах для установки в документе «Руководство оператора», раздел «Работа с наборами для установки»

³¹ Проверить, является ли конвейер главным, можно в приложении Ankey SIEM NG → Система → Управление системой → Конвейеры на боковой панели справа.

9. Нажмите кнопку **Создать**.
Набор для установки создан.
10. В панели **Наборы для установки** выберите **Все объекты**.
11. В панели **Папки** выберите необходимый пакет экспертизы (или папку).
Появится список объектов пакета экспертизы (папки).
12. Выберите необходимые объекты.

Примечание. Содержимое набора для установки следует формировать с учетом того, что при установке новых ресурсов в компонент Server ресурсы, которые были установлены ранее, автоматически и принудительно удаляются, а новые устанавливаются.

Поэтому набор для установки должен содержать полный набор необходимых правил нормализации, корреляции, обогащения, агрегации и табличных списков без учета установленных ранее ресурсов.

Внимание! В случае использования схемы «горизонтальный SIEM» при установке ресурсов в конвейеры необходимо всегда добавлять в набор установки следующие табличные списки из пакета общих ресурсов контента:

- COMMON_Tracking_Exceptions
- COMMON_Hosts_Configuration
- COMMON_Users_Configuring
- COMMON_Files_Forbidden
- COMMON_Hosts_Scada_Zone
- COMMON_VIRT_Critical_VM

Если это условие не будет выполнено, установка ресурсов завершится ошибкой.

13. Нажмите на графическую кнопку .
Откроется окно **Наборы для установки**.
14. Установите флажок напротив названия набора для установки, в который нужно добавить объекты.

Примечание. Место ресурса в иерархической структуре не поменяется, наборы для установки представляют собой группы, которые объединяют объекты по некоторому признаку.

15. Нажмите кнопку **Сохранить**.
Объекты добавлены в набор для установки.
16. Из набора установки необходимо удалить все родительские ресурсы, с которых были созданы копии в ветке **Customer_Data**, чтобы не было конфликтов в работе SIEM-системы после установки. Найти родительский ресурс, выделив скопированный, возможно, перейдя к нему по ссылке из описания скопированного ресурса в панели справа, как показано на рисунке 3.22).

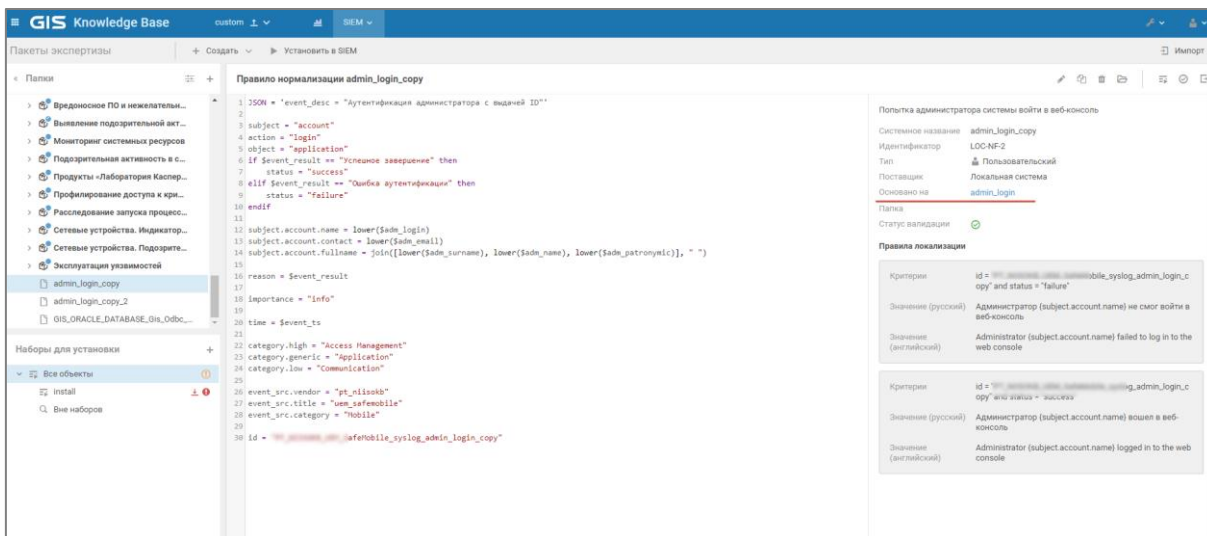


Рисунок 3.22 – Ссылка на родительский ресурс

17. Установить контент в компонент Ankey SIEM NG Server, нажав на графическую кнопку ►. Начнется установка контента.

Примечание. При наведении курсора на значок ► во всплывающей подсказке отображается статус установки.

18. После завершения установки в рабочей области появится сообщение Установка успешно завершена. Контент установлен из Knowledge Base в Ankey SIEM NG Server.

3.15 Установка компонента Ankey SIEM NG Collector

В этом подразделе приведены инструкции по установке компонента Ankey SIEM NG Collector на Linux и на Microsoft Windows. Установка компонента на Linux выполняется с помощью роли Collector.

Если Ankey SIEM NG Collector устанавливается на Linux и на этом сервере уже установлен Kaspersky Endpoint Security, необходимо обновить антивирусные базы Kaspersky Endpoint Security и включить компонент Kaspersky Security Network (KSN).

Если в процессе установки ОС Astra Linux 1.7.x было установлено ПО Средства работы в сети, то перед установкой Ankey SIEM NG Collector необходимо установить пакет libsassl2-modules-gssapi-mit с помощью команды apt install libsassl2-modules-gssapi-mit. Если не установить пакет libsassl2-modules-gssapi-mit, то установка Ankey SIEM NG Collector не будет успешно выполнена.

3.15.1 Установка модуля Salt Minion на сервер Ankey SIEM NG Collector

Внимание! Для средненагруженных и высоконагруженных систем на сервере, на который устанавливается модуль Salt Minion, порт 22/TCP должен быть открыт для входящих соединений.

Если Ankey SIEM NG Collector устанавливается на отдельный сервер, перед установкой роли необходимо установить на этот сервер модуль Salt Minion. Если на сервере, на котором разворачивается компонент, уже установлена роль Deployer, установка модуля Salt Minion не требуется.

Чтобы установить модуль Salt Minion:

1. Если на сервере Ankey SIEM NG Collector есть файл `/etc/salt/pki/minion/minion_master.pub`, удалите его:
`rm /etc/salt/pki/minion/minion_master.pub`
2. Если Ankey SIEM NG Collector устанавливается на Astra Linux, на сервере Ankey SIEM NG Collector отключите обязательный ввод пароля для выполнения команды `sudo`:
`sudo astra-sudo-control disable`
3. Если Ankey SIEM NG Collector устанавливается на Debian, на сервере компонента установите утилиту `sudo`, выполнив в интерфейсе терминала команду от имени суперпользователя (`root`):
`apt-get install sudo`
4. Если Ankey SIEM NG Collector устанавливается на Debian, на сервере компонента отключите обязательный ввод пароля для выполнения команды `sudo`, добавив в файл `/etc/sudoers` строку:
<Логин учетной записи, от имени которой устанавливается компонент>
`ALL=(ALL:ALL) NOPASSWD: ALL`
5. На сервере с установленной ролью Deployer запустите сценарий:
`/var/lib/deployer/role_packages/deployer_<Номер версии>/deploy_minion.sh`
6. В открывшемся окне введите полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Collector и нажмите кнопку **ОК**.

Внимание! Если в окне указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

7. В открывшемся окне введите логин учетной записи, от имени которой устанавливается компонент, на сервере Ankey SIEM NG Collector и нажмите кнопку **ОК**.
8. В открывшемся окне **Info** нажмите кнопку **ОК**.
9. Введите пароль учетной записи с правами суперпользователя на сервере Ankey SIEM NG Collector.
10. Если требуется, в открывшемся окне введите FQDN или IPv4-адрес сервера и нажмите кнопку **ОК**.

По завершении установки появится сообщение `Minion on '<FQDN или IPv4-адрес сервера>' successfully installed.`

Модуль Salt Minion установлен.

3.15.2 Установка роли Collector

Для установки роли вам потребуется архив `agent-linux_<Номер версии>.tar.gz` из комплекта поставки.

Чтобы установить роль:

1. На сервере с установленной ролью **Deployer** распакуйте архив `agent-linux_<Номер версии>.tar.gz`:
`tar -xf agent-linux_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для установки.
По завершении подготовки откроется окно для выбора приложения.
4. Выполните одно из следующих действий:
 - если в открывшемся окне для выбора доступен вариант с идентификатором установленного ранее приложения **Ankey SIEM NG** – выберите этот вариант;
 - если вариант с идентификатором установленного ранее приложения **Ankey SIEM NG** отсутствует – выберите вариант **Create New Application**.
5. Если вы выбрали вариант **Create New Application**, в открывшемся окне введите идентификатор приложения **Ankey SIEM NG** и нажмите кнопку **OK**.
6. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.
7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем сервера **Ankey SIEM NG Collector**.
9. В открывшемся окне введите название экземпляра роли **Collector** и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
10. Выберите вариант **Advanced configuration**.
Откроется страница со списком параметров.
11. В качестве значения параметра `AgentName` введите название коллектора, которое будет отображаться в веб-интерфейсе приложения **Ankey SIEM NG**.
12. Убедитесь, что в качестве значения параметра `AgentRMQHost` указано полное доменное имя (FQDN) или IPv4-адрес стандартной или облегченной версии **Ankey SIEM NG Server** – в зависимости от того, для какой версии компонента предназначен **Ankey SIEM NG Collector**.

Внимание! Если в параметре `AgentRMQHost` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

13. В качестве значения параметра `AgentRMQVirtualHost` выберите **SIEM**.
14. Нажмите кнопку **ОК**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
15. Нажмите кнопку **ОК**.
16. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль установлена.

Примечание. Для корректной работы Ankey SIEM NG Collector в ОС Linux требуется отдельно скачать и установить ODBC-драйвер (версия для 64-разрядной архитектуры) для требуемых источников, которые будут подключаться к ПК Ankey SIEM NG. Драйвер вы можете скачать с официальных сайтов производителей источников.

3.16 Установка компонента Ankey SIEM NG Collector на Microsoft Windows

Для установки компонента Ankey SIEM NG Collector на Microsoft Windows вам потребуется архив `agent-windows_<Номер версии>.tar.gz` из комплекта поставки.

Чтобы установить компонент Ankey SIEM NG Collector:

1. Запустите файл `AnkeyAgentSetup_<Номер версии>.exe`.
Откроется окно мастера установки.
2. Ознакомьтесь по ссылке с текстом лицензионного соглашения.
3. Установите флажок **Я принимаю условия лицензионного соглашения** и нажмите кнопку **Продолжить**.
4. Укажите пути для установки.

Примечание. Если вы хотите установить компоненты в папки по умолчанию, не изменяйте значения полей.

5. Нажмите кнопку **Продолжить**.
6. В поле **Имя коллектора** введите имя коллектора, которое будет отображаться в интерфейсе ПК Ankey SIEM NG.
7. В блоке параметров **Адрес обработчика данных** в раскрывающемся списке выберите значение **SIEM** и укажите в поле полное доменное имя (FQDN) или IPv4-адрес стандартной или облегченной версии Ankey SIEM NG Server – в зависимости

от того, для какой версии компонента предназначен Ankey SIEM NG Collector.

Внимание! Если в поле указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

8. Нажмите кнопку **Продолжить**.
Мастер установки выполнит проверку указанных вами параметров и отобразит их после проверки.

Примечание. По результатам проверки мастер может отображать сообщения о некорректных значениях указанных параметров. Вам необходимо вернуться, нажимая кнопку **Назад**, и указать корректные значения параметров.

9. Нажмите кнопку **Установить**.
10. По завершении установки нажмите кнопку **Заккрыть**.
11. Если устанавливается первый компонент Ankey SIEM NG Collector и компонент Ankey SIEM NG Server установлен на Linux, на сервере с установленной ролью Deployer выполните команды:
 - `cp /opt/deployer/pki/legacy_ca/windows-selfsigned-default.pem /opt/deployer/pki/trusted_ca/`
 - `dpkg-reconfigure deployer`
 - `/opt/deployer/bin/Restart-Configuration.ps1 -RoleTypeId RmqMessageBus`
 - `/opt/deployer/bin/Restart-Configuration.ps1 -RoleTypeId SiemServer`
12. Если первый компонент Ankey SIEM NG Collector устанавливается на Windows, перезапустите службу Core Collector.
13. Для подключения модуля Salt Minion к модулю Salt Master выполните команду:
`saltcfg set -p SaltMasterHost <IP-адрес или FQDN сервера с модулем Salt Master>`

Компонент Ankey SIEM NG Collector установлен.

3.17 Установка облегченной версии компонента Ankey SIEM NG Server на Linux

Перед установкой облегченной версии Ankey SIEM NG Server необходимо установить компонент Ankey SIEM NG Collector. Также необходимо убедиться, что в качестве значения параметра `AgentRMQHost` компонента Ankey SIEM NG Collector указан FQDN или IPv4-адрес сервера облегченной версии Ankey SIEM NG Server, а параметру `AgentRMQVirtualHost` присвоено значение `siem`.

Внимание! Не предусмотрено развертывание облегченной версии Ankey SIEM NG Server на том же сервере, где установлен компонент Ankey SIEM NG Core.

Установка облегченной версии компонента Ankey SIEM NG Server делится на следующие этапы:

1. Установка модуля Salt Minion.

Внимание! Если на сервере, на котором развертывается компонент, уже установлена роль `Deployer`, установка модуля Salt Minion не требуется.

2. Установка роли `RMQ Message Bus`.
3. Установка роли `SIEM Server`.

3.17.1 Установка модуля Salt Minion на сервер облегченной версии Ankey SIEM NG Server

Внимание! Для средненагруженных и высоконагруженных систем на сервере, на который устанавливается модуль Salt Minion, порт 22/TCP должен быть открыт для входящих соединений.

Чтобы установить модуль Salt Minion:

1. Если на сервере облегченной версии Ankey SIEM NG Server есть файл `/etc/salt/pki/minion/minion_master.pub`, удалите его:
`rm /etc/salt/pki/minion/minion_master.pub`
2. Если облегченная версия Ankey SIEM NG Server устанавливается на сервер на Astra Linux, отключите на этом сервере обязательный ввод пароля для выполнения команды `sudo`:
`sudo astra-sudo-control disable`
3. Если облегченная версия Ankey SIEM NG Server устанавливается на Debian, на сервере компонента установите утилиту `sudo`, выполнив в интерфейсе терминала команду от имени суперпользователя (`root`):
`apt-get install sudo`
4. Если облегченная версия Ankey SIEM NG Server устанавливается на Debian, на сервере компонента отключите обязательный ввод пароля для выполнения команды `sudo`, добавив в файл `/etc/sudoers` строку:

<Логин учетной записи, от имени которой устанавливается компонент>
ALL=(ALL:ALL) NOPASSWD: ALL

5. На сервере с установленной ролью Deployer запустите сценарий:
/var/lib/deployer/role_packages/deployer_<Номер версии>/deploy_minion.sh
6. В открывшемся окне введите FQDN или IPv4-адрес сервера облегченной версии Ankey SIEM NG Server и нажмите кнопку **OK**.

Внимание! Если в окне указать значение localhost, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

7. В открывшемся окне введите логин учетной записи, от имени которой устанавливается компонент, на сервере облегченной версии Ankey SIEM NG Server и нажмите кнопку **OK**.
8. В окне **Info** нажмите кнопку **OK**.
9. Введите пароль учетной записи с правами суперпользователя (root) на сервере облегченной версии Ankey SIEM NG Server. Запустится установка модуля Salt Minion.
10. Если требуется, в открывшемся окне введите FQDN или IPv4-адрес сервера и нажмите кнопку **OK**.
По завершении установки появится сообщение Minion on '<FQDN или IPv4-адрес сервера>' successfully installed.

Модуль Salt Minion установлен.

3.17.2 Установка роли RMQ Message Bus на сервер облегченной версии Ankey SIEM NG Server

Для установки роли вам потребуется архив rmqmessagebus_<Номер версии>.tar.gz из комплекта поставки.

Чтобы установить роль:

1. На сервере с установленной ролью Deployer распакуйте архив rmqmessagebus_<Номер версии>.tar.gz:
tar -xvf rmqmessagebus_<Номер версии>.tar.gz
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли ./install.sh.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В окне **Instance selection** выберите вариант **Deploy New Instance**.
6. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. В открывшемся окне выберите вариант с доменным именем сервера облегченной версии Ankey SIEM NG Server.
8. В открывшемся окне введите название экземпляра роли RMQ Message Bus и нажмите кнопку **OK**.

- Откроется окно для проверки и изменения параметров установки.
9. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.
 10. Укажите в качестве значения параметра HostAddress FQDN или IPv4-адрес сервера облегченной версии Ankey SIEM NG Server.

Внимание! Если в параметре HostAddress указать значение localhost, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

11. Нажмите кнопку **ОК**.
Начнется установка пакетов. По завершении установки появится сообщение Deployment configuration successfully applied.
12. Нажмите кнопку **ОК**.
Роль установлена.

3.17.3 Установка роли SIEM Server для облегченной версии компонента

Для установки роли вам потребуется архив `siemserver-linux_<Номер версии>.tar.gz` из комплекта поставки.

Чтобы установить роль:

1. На сервере с установленной ролью **Deployer** распакуйте архив `siemserver-linux_<Номер версии>.tar.gz`:
`tar -xvf siemserver-linux_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения **Ankey SIEM NG**.
5. В окне **Instance selection** выберите вариант **Deploy New Instance**.
6. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. В открывшемся окне выберите вариант с доменным именем сервера **Ankey SIEM NG Server**.
8. В открывшемся окне введите название экземпляра роли **SIEM Server** и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
9. Выберите набор параметров **Advanced configuration**.
Откроется страница с перечнем всех доступных параметров конфигурации.

Внимание! Укажите значения параметров:

`HostAddress`: <FQDN или IPv4-адрес сервера облегченной версии компонента Ankey SIEM NG Server>

`TargetSiemRabbitHost`: <FQDN или IPv4-адрес сервера Ankey SIEM NG Server, который будет получать данные о событиях от облегченной версии компонента>

Внимание! Если в параметрах указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

10. Установите флажок **SiemOnAgent**.
11. Если ПК Ankey SIEM NG развертывается в конфигурации для высоконагруженных систем с потоком событий выше 20000 событий в секунду, установите флажок **ManagedStorage**.
12. Нажмите кнопку **OK**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
13. Нажмите кнопку **OK**.

14. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.
Роль установлена.

3.18 Установка облегченной версии компонента Ankey SIEM NG Server на Microsoft Windows

Перед установкой облегченной версии компонента Ankey SIEM NG Server необходимо установить на том же сервере компонент Ankey SIEM NG Collector. Чтобы установить облегченную версию Ankey SIEM NG Server:

1. Распакуйте архив `siemserver-windows_<Номер версии>.tar.gz`
2. Скопируйте файл `AnkeySiemSetup_<Номер версии>.exe` на сервер облегченной версии Ankey SIEM NG Server.
3. Запустите файл `AnkeySiemSetup_<Номер версии>.exe`.
Откроется окно мастера установки.
4. Ознакомьтесь по ссылке с текстом лицензионного соглашения.
5. Установите флажок **Я принимаю условия лицензионного соглашения** и нажмите кнопку **Продолжить**.
6. Выберите вариант установки облегченной версии Ankey SIEM NG Server и нажмите кнопку **Продолжить**.
7. Укажите пути для установки.

Примечание. Если вы хотите установить компоненты в папки по умолчанию, не изменяйте значения полей.

8. Нажмите кнопку **Продолжить**.
Мастер установки выполнит проверку указанных вами параметров и отобразит их после проверки.

Примечание. По результатам проверки мастер может отображать сообщения о некорректных значениях указанных параметров. В этом случае вам необходимо вернуться, нажимая кнопку **Назад**, и указать корректные значения параметров.

9. Нажмите кнопку **Установить**.
10. По завершении установки нажмите кнопку **Заккрыть**.
11. Если стандартная версия Ankey SIEM NG Server установлена на Linux, скопируйте файл `/opt/deployer/pki/CABundle.crt` с сервера, на котором установлена роль Deployer, на сервер облегченной версии Ankey SIEM NG Server.
12. Если стандартная версия Ankey SIEM NG Server установлена на Linux, скопируйте файлы `/var/lib/deployed-roles/<Идентификатор приложения Ankey SIEM NG Server>/<Название экземпляра роли SIEM Server>/certs/RMQ_SIEM_Client.crt` и `/var/lib/deployed-roles/<Идентификатор приложения Ankey SIEM NG Server>/<Название экземпляра роли SIEM Server>/certs/RMQ_SIEM_Client.key` с сервера стандартной версии Ankey SIEM NG Server на сервер облегченной версии Ankey SIEM NG Server.

На сервере облегченной версии Ankey SIEM NG Server в интерфейсе командной строки Windows от имени администратора выполните команды:

```
coreagentcfg set -p AgentRMQVirtualHost siem RMQHost localhost
rabbitmqcfg set -p CACertFile <Путь к файлу CABundle.crt> -v
siemcfg set -p TargetSiemRabbitHost <FQDN или IPv4-адрес стандартной
версии Ankey SIEM NG Server> RMQHost <FQDN или IPv4-адрес
стандартной версии Ankey SIEM NG Server> RMQ_SSL_CA_CERTIFICATE
<Путь к файлу CABundle.crt> RMQ_SSL_CERTIFICATE <Путь к файлу
RMQ_SIEM_Client.crt> RMQ_SSL_KEY <Путь к файлу
RMQ_SIEM_Client.key>
```

Облегченная версия компонента Ankey SIEM NG Server установлена.

После установки облегченной версии компонента Ankey SIEM NG Server необходимо установить правила нормализации и агрегации (см. раздел 3.19).

3.19 Установка правил нормализации и агрегации для облегченной версии Ankey SIEM NG Server

Установка правил нормализации и агрегации для облегченной версии Ankey SIEM NG Server происходит автоматически при установке ресурсов из Knowledge Base в основной конвейер обработки данных. Инструкции по установке стандартной базы данных представлены в подразделе 3.14.

3.20 Установка дополнительного компонента Ankey SIEM NG RC

Внимание! Компонент Ankey SIEM NG RC необходимо устанавливать на отдельный сервер, отличный от серверов Ankey SIEM NG Server и Ankey SIEM NG Collector.

Установка компонента Ankey SIEM NG RC делится на следующие этапы:

1. Установка модуля Salt Minion.

Внимание! Если на сервере, на котором разворачивается компонент, уже установлена роль Deployer, установка модуля Salt Minion не требуется.

2. Установка роли RMQ Message Bus.
3. Установка роли Retro Correlator.

3.20.1 Установка модуля Salt Minion на сервер Ankey SIEM NG RC

Внимание! Для средненагруженных и высоконагруженных систем на сервере, на который устанавливается модуль Salt Minion, порт 22/TCP должен быть открыт для входящих соединений.

Чтобы установить модуль Salt Minion:

1. Если на сервере Ankey SIEM NG RC есть файл `/etc/salt/pki/minion/minion_master.pub`, удалите его:
`rm /etc/salt/pki/minion/minion_master.pub`
2. Если Ankey SIEM NG RC устанавливается на Astra Linux, на сервере Ankey SIEM NG RC отключите обязательный ввод пароля для выполнения команды `sudo`:
`sudo astra-sudo-control disable`
3. Если Ankey SIEM NG RC устанавливается на Debian, на сервере компонента установите утилиту `sudo`, выполнив в интерфейсе терминала команду от имени суперпользователя (root):
`apt-get install sudo`
4. Если Ankey SIEM NG RC устанавливается на Debian, на сервере компонента отключите обязательный ввод пароля для выполнения команды `sudo`, добавив в файл `/etc/sudoers` строку:
<Логин учетной записи, от имени которой устанавливается компонент>
`ALL=(ALL:ALL) NOPASSWD: ALL`
5. На сервере с установленной ролью Deployer запустите сценарий:
`/var/lib/deployer/role_packages/Deployer_<Номер версии>/deploy_minion.sh`
6. В открывшемся окне введите полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG RC и нажмите кнопку **ОК**.

Внимание! Если в окне указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

7. В открывшемся окне введите логин учетной записи, от имени которой устанавливается компонент, на сервере Ankey SIEM NG RC и нажмите кнопку **ОК**.
8. В открывшемся окне **Info** нажмите кнопку **ОК**.
9. Введите пароль учетной записи с правами суперпользователя на сервере Ankey SIEM NG RC.
Запустится установка модуля Salt Minion.
10. Если требуется, в открывшемся окне введите FQDN или IPv4-адрес сервера и нажмите кнопку **ОК**.
По завершении установки появится сообщение `Minion on '<FQDN или IPv4-адрес сервера >' successfully installed..`

Модуль Salt Minion установлен.

3.20.2 Установка роли RMQ Message Bus на сервер Ankey SIEM NG RC

Для установки роли вам потребуется архив `rmqmessagebus_<Номер версии>.tar.gz` из комплекта поставки.

Чтобы установить роль:

1. На сервере с установленной ролью **Deployer** распакуйте архив `rmqmessagebus_<Номер версии>.tar.gz`:
`tar -xvf rmqmessagebus_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для установки.
По завершении подготовки откроется окно для выбора приложения.
4. Выполните одно из следующих действий:
 - если в открывшемся окне для выбора доступен вариант с идентификатором установленного ранее приложения Ankey SIEM NG – выберите этот вариант;
 - если вариант с идентификатором установленного ранее приложения Ankey SIEM NG отсутствует – выберите вариант **Create New Application**.
5. Если вы выбрали вариант **Create New Application**, в открывшемся окне введите идентификатор приложения Ankey SIEM NG и нажмите кнопку **OK**.
6. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.
7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG RC.
9. В открывшемся окне введите название экземпляра роли RMQ Message Bus и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
10. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.
11. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG RC.

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

12. Нажмите кнопку **OK**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
13. Нажмите кнопку **OK**.

14. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.
Роль установлена.

3.20.3 Установка роли Retro Correlator

Для установки роли вам потребуется архив `retrocorrelator_<Номер версии>.tar.gz` из комплекта поставки.

Чтобы установить роль:

1. На сервере с установленной ролью **Deployer** распакуйте архив `retrocorrelator_<Номер версии>.tar.gz`:
`tar -xf retrocorrelator_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выберите вариант с идентификатором приложения **Ankey SIEM NG**.
5. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.

Внимание! Можно создать только один экземпляр (Instance).

6. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. В открывшемся окне выберите вариант с доменным именем сервера **Ankey SIEM NG RC**.
8. В открывшемся окне введите название экземпляра роли **Retro Correlator** и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
9. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.

Внимание! Укажите значения параметров:

AgentName: <Название коллектора, которое будет отображаться в веб-интерфейсе приложения Ankey SIEM NG>
AgentRMQHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Server>
AgentRMQVirtualHost: SIEM
HostAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG RC>
InternalRMQHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG RC>
CoreAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>
KBAddress: < FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:8091
SiemServerAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Server>

Внимание! Если в параметрах указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

10. Нажмите кнопку **ОК**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
11. Нажмите кнопку **ОК**.
Роль установлена.

3.21 Установка доверенного сертификата для сайта ПК Ankey SIEM NG

При разворачивании ПК Ankey SIEM NG для его сайта автоматически устанавливается самоподписанный сертификат, поставляемый в составе дистрибутива. Поэтому при попытке подключения к сайту вы получите предупреждение о том, что создаваемое подключение не защищено.

Вы можете установить собственный доверенный сертификат, который должен отвечать следующим требованиям:

- использовать алгоритм подписи SHA-256;
- использовать алгоритм шифрования ключей RSA;
- соответствовать формату PEM;
- иметь заголовок `BEGIN CERTIFICATE` без дополнительных заголовков;
- содержать закрытый незашифрованный ключ в формате PEM длиной не менее 2048 бит с заголовком `BEGIN RSA PRIVATE KEY` без дополнительных заголовков;

Примечание. Чтобы расшифровать зашифрованный с помощью алгоритма RSA ключ, необходимо выполнить команду `openssl rsa -in encrypted.key -out decrypted.key`.

- включать область применения сертификата `Digital Signature` или `Key Encipherment`;
- в расширении `Extended Key Usage (EKU)` содержать записи `serverAuth` и `clientAuth`;
- в расширении `Subject Alternative Name (SAN)` содержать запись об FQDN сервера компонента или его IP-адресе в зависимости от значения параметра `HostAddress` (оно может быть равно как FQDN, так и IP-адресу).

Чтобы установить доверенный сертификат на Linux:

1. На сервере Ankey SIEM NG Core разместите файлы сертификата и закрытого ключа в каталогах `/var/lib/deployed-roles/<Идентификатор приложения Ankey SIEM NG>/<Название экземпляра роли>/certs` для каждой роли `Core`, `Management and Configuration` и `Knowledge Base`.

2. На сервере с установленной ролью Deployer разместите файлы сертификатов центров сертификации всей цепочки в каталоге /opt/deployer/pki/trusted_ca/.
3. Выполните команду:
dpkg-reconfigure deployer
4. Измените конфигурации (см. документ «Руководство администратора Ankey SIEM NG, раздел «Просмотр и изменение параметров конфигурации Ankey SIEM NG») ролей Core, Management and Configuration и Knowledge Base.
SSLCertificatePemFileName: <Имя файла сертификата>
SSLKeyFileName: <Имя файла закрытого ключа>
Например:
SSLCertificatePemFileName: website.crt
SSLKeyFileName: website.key
Сертификат установлен.

Внимание! Имена файлов сертификата и ключа не должны совпадать с именами файлов, которые уже находятся в папке сертификатов: замена содержимого стандартных файлов приведет к некорректной работе системы.

3.22 Установка пользовательского сертификата для RMQ Message Bus и компонентов Ankey SIEM NG Core, Ankey SIEM NG Server и Ankey SIEM NG Collector

Для RMQ Message Bus и компонентов Ankey SIEM NG Core, Ankey SIEM NG Server и Ankey SIEM NG Collector вы можете установить пользовательский сертификат безопасности, который должен отвечать следующим требованиям:

- использовать алгоритм подписи SHA-256;
- использовать алгоритм шифрования ключей RSA;
- соответствовать формату PEM;
- использовать отдельные файлы для хранения сертификата центра сертификации (ЦС), пользовательского сертификата и закрытого ключа;
- иметь заголовок BEGIN CERTIFICATE без дополнительных заголовков;
- содержать закрытый незашифрованный ключ в формате PEM длиной не менее 2048 бит с заголовком BEGIN RSA PRIVATE KEY без дополнительных заголовков;

Примечание. Чтобы расшифровать зашифрованный с помощью алгоритма RSA ключ, необходимо выполнить команду `openssl rsa -in encrypted.key -out decrypted.key`.

- включать область применения сертификата Digital Signature или Key Encipherment;

- содержать в расширении Extended Key Usage (EKU) записи аутентификации сервера `serverAuth` и аутентификации клиента `clientAuth`;
- содержать в поле `Common Name` значения `core`, `siem` или `agent` для компонентов Ankey SIEM NG Core, Ankey SIEM NG Server и Ankey SIEM NG Collector соответственно.

Чтобы установить пользовательский сертификат RMQ Message Bus и компонентов Ankey SIEM NG Core, Ankey SIEM NG Server и Ankey SIEM NG Collector на Linux:

1. Разместите файлы сертификата ЦС, пользовательского сертификата и закрытого ключа в каталогах `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs` для ролей RMQ Message Bus, Core, SIEM Server и Agent.
2. Измените конфигурацию роли RMQ Message Bus:
`CACertFile: <Имя файла сертификата ЦС>`
`CertFile: <Имя файла пользовательского сертификата>`
`KeyFile: <Имя файла закрытого ключа>`
3. Измените конфигурацию роли Core:
`CACertificateFileName: <Имя файла сертификата ЦС>`
`RMQSSLCertificateFileName: <Имя файла пользовательского сертификата>`
`RMQSSLKeyFileName: <Имя файла закрытого ключа>`
4. Измените конфигурацию роли SIEM Server:
`RMQ_SSL_CA_CERTIFICATE: <Полный путь к файлу сертификата ЦС>`
`RMQ_SSL_CERTIFICATE: <Полный путь к файлу пользовательского сертификата>`
`RMQ_SSL_KEY: <Полный путь к файлу закрытого ключа>`
5. Измените конфигурацию роли Collector:
`Agent_RMQ_SSL_CA_Certificate: <Полный путь к файлу сертификата ЦС>`
`Agent_RMQ_SSL_Certificate: <Полный путь к файлу пользовательского сертификата>`
`Agent_RMQ_SSL_Key: <Полный путь к файлу закрытого ключа>`

Сертификат установлен.

3.23 Настройка обновления экспертных данных

Примечание. Работа с экспертными данными доступна только в исполнениях Ankey SIEM NG VM и Ankey SIEM NG с дополнительным компонентом VM.

Автоматическое обновление экспертных данных в Ankey SIEM NG с компонентом VM осуществляется с помощью сервиса Package Management, который входит в состав компонента Ankey SIEM NG MC. Сервис получает пакеты обновлений с глобального сервера обновлений³² напрямую или через локальный сервер обновлений Ankey Update Mirror и устанавливает их в продукты с соответствующими лицензиями. Такой способ обновления стал возможен благодаря переходу на новую модель хранения экспертных данных.

Внимание! Процесс миграции на новую модель хранения экспертных данных является обязательным при обновлении ПК Ankey SIEM NG 5.2.3 с версии 4.x на версию 5.x и необходим для корректной работы системы и получения обновлений экспертных данных. Миграция запускается после обновления Ankey SIEM NG.

Для миграции на новую модель хранения экспертных данных после обновления роли Management and Configuration необходимо из комплекта поставки скопировать файл миграционного пакета данных с названием вида migration.vm.s.1.0.v.<Версия пакета данных>.pkg и разместить его на сервере с ролью Management and Configuration в каталоге /var/lib/deployed-roles/mc-application-ankey/managementandconfiguration/data/resources/local-packages/.

Внимание! Файл миграционного пакета необходимо разместить в каталоге в течение 24 часов с момента начала обновления системы.

³² Доступ к обновлениям предоставляется через официальный сайт update.ptsecurity.com в рамках партнёрства с вендором пакетов обновлений

3.23.1 Схемы получения обновлений экспертных данных, поддерживаемые Ankey SIEM NG

Порядок настройки подключения к серверу обновлений зависит от размещения Ankey SIEM NG в инфраструктуре компании.

1. Получение обновлений напрямую с глобального сервера обновлений

Схема получения обновлений напрямую доступна в случае, если ПК Ankey SIEM NG доступно прямое подключение к интернету (рисунок 3.23).

Для получения обновлений необходимо:

- при установке (см. подраздел 3.7.5) или обновлении роли Management and Configuration (см. подраздел 4.1.2.3) указать значения параметров ExpertDataUpdateMethod, PackagesSourceUri и PackagesSourceCredentialToken. Если роль Management and Configuration уже установлена, укажите значения параметров в соответствии с инструкцией (см. раздел 3.23.3).

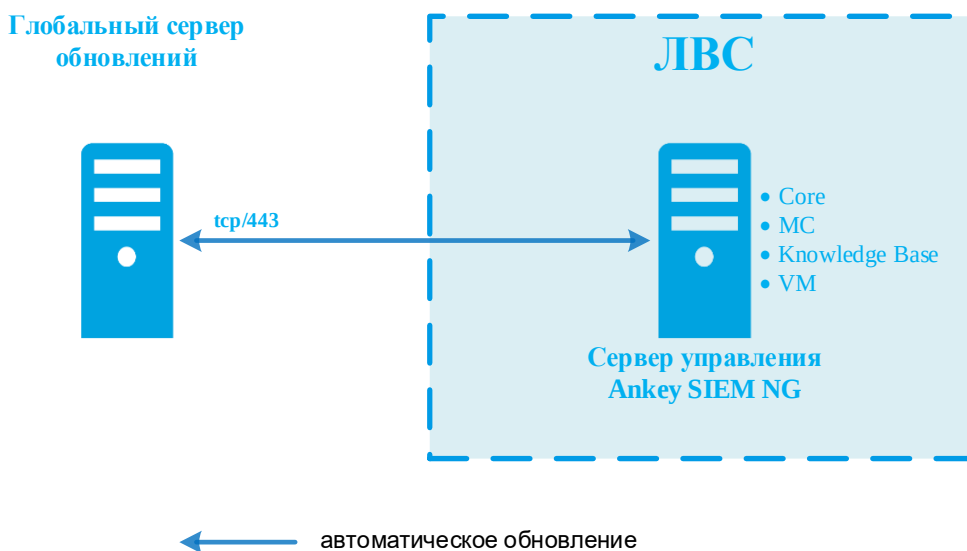


Рисунок 3.23 – Схема получения обновлений напрямую с глобального сервера обновлений

2. Получение обновлений через локальный сервер обновлений, который установлен в изолированном сегменте локальной сети

В случае, если ПК Ankey SIEM NG установлен в изолированном сегменте локальной сети организации и доступ в демилитаризованную зону (далее также – DMZ) отсутствует, вы можете развернуть и настроить в изолированном сегменте локальной сети организации локальный сервер обновлений Ankey Update Mirror, который будет подключаться к глобальному серверу обновлений через прокси-сервер (рисунок 3.24). Он будет загружать обновления с глобального сервера обновлений и передавать их в изолированный сегмент сети.

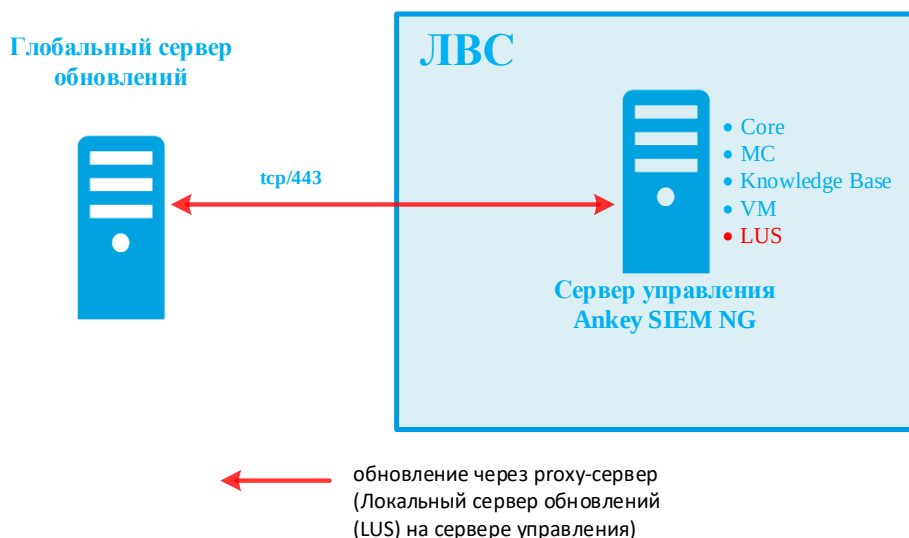


Рисунок 3.24 – Схема получения обновлений через локальный сервер обновлений

Для получения обновлений необходимо:

- при установке (см. подраздел 3.7.5) или обновлении роли Management and Configuration (см. подраздел 4.1.2.3) указать значения параметров ExpertDataUpdateMethod, PackagesSourceUri и PackagesSourceCredentialToken;
- Настроить подключение локального сервера обновлений к прокси-серверу (см. подраздел 3.23.7).

3. Получение обновлений через локальный сервер обновлений Ankey Update Mirror, установленный в демилитаризованной зоне.

В случае, если ПК Ankey SIEM NG установлен в изолированном сегменте сети организации и имеет доступ в демилитаризованную зону, вы можете развернуть и настроить в демилитаризованной зоне локальный сервер обновлений Ankey Update Mirror, который будет подключаться к глобальному серверу обновлений напрямую или через прокси-сервер (рисунок 3.25). Он будет загружать обновления с глобального сервера обновлений и передавать их в изолированный сегмент сети.

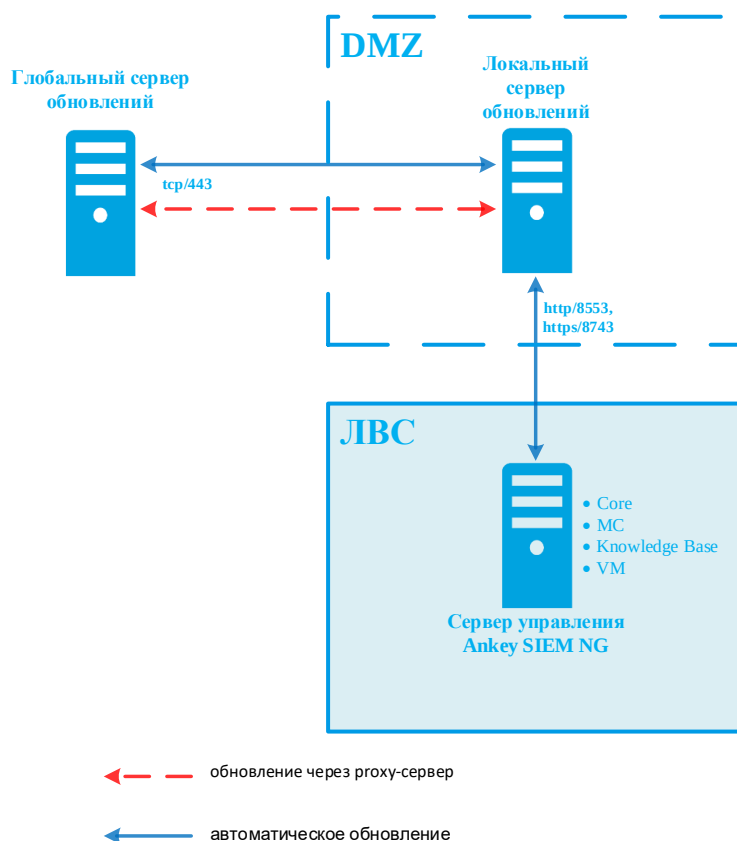


Рисунок 3.25 – Схема получения обновлений с одним Ankey Update Mirror, установленным в демилитаризованной зоне

Для получения обновлений необходимо:

- при установке (см. подраздел 3.7.5) или обновлении роли Management and Configuration (см. подраздел 4.1.2.3) указать значения параметров ExpertDataUpdateMethod, PackagesSourceUri и PackagesSourceCredentialToken;
- установить в демилитаризованной зоне локальный сервер обновлений;
- если требуется, настроить подключение локального сервера обновлений к прокси-серверу (см. подраздел 3.23.7);
- активировать лицензию локального сервера обновлений.

4. Получение обновлений через два локальных сервера обновлений Ankey Update Mirror, установленных в закрытом сегменте сети и демилитаризованной зоне.

В случае, если ПК Ankey SIEM NG установлен в изолированном от интернета сегменте сети и не должен иметь выход в демилитаризованную зону, вы можете использовать схему обновления с двумя локальными серверами обновлений:

- первый локальный сервер обновлений Ankey Update Mirror установлен в изолированном сегменте сети, где находится Ankey SIEM NG. Установка этого локального сервера Ankey Update Mirror возможна в двух вариантах:
 - **вариант 1** – Ankey Update Mirror установлен на сервере управления (рисунок 3.26);
 - **вариант 2** – Ankey Update Mirror установлен на отдельном сервере (рисунок 3.27).
- второй локальный сервер обновлений Ankey Update Mirror находится в демилитаризованной зоне. Локальный сервер обновлений в демилитаризованной зоне будет загружать обновления с глобального сервера обновлений.

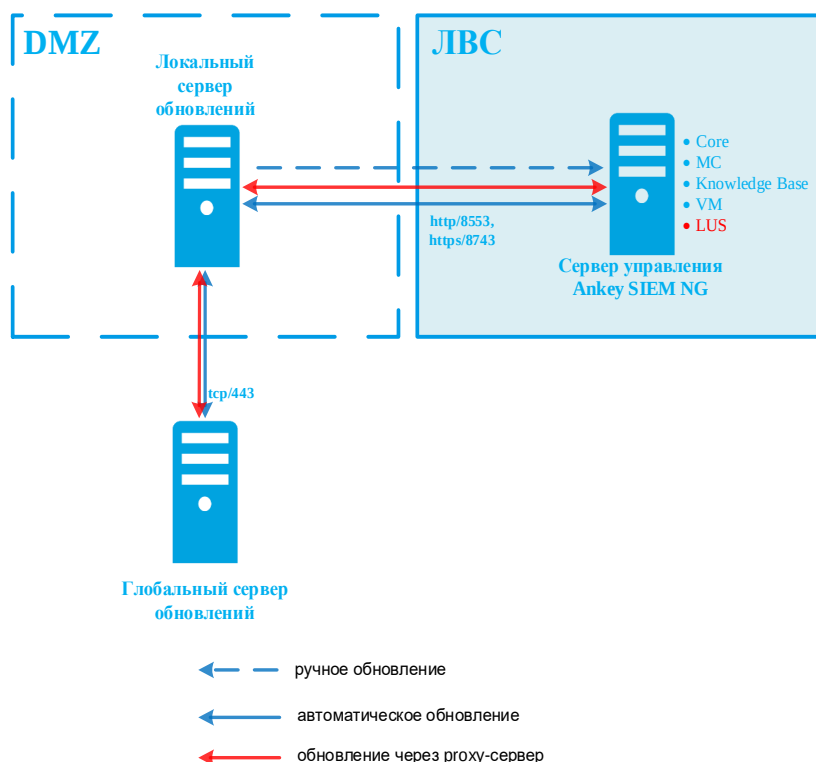


Рисунок 3.26 – Схема получения обновлений с двумя Ankey Update Mirror, установленными в закрытом сегменте сети и в демилитаризованной зоне (вариант 1)

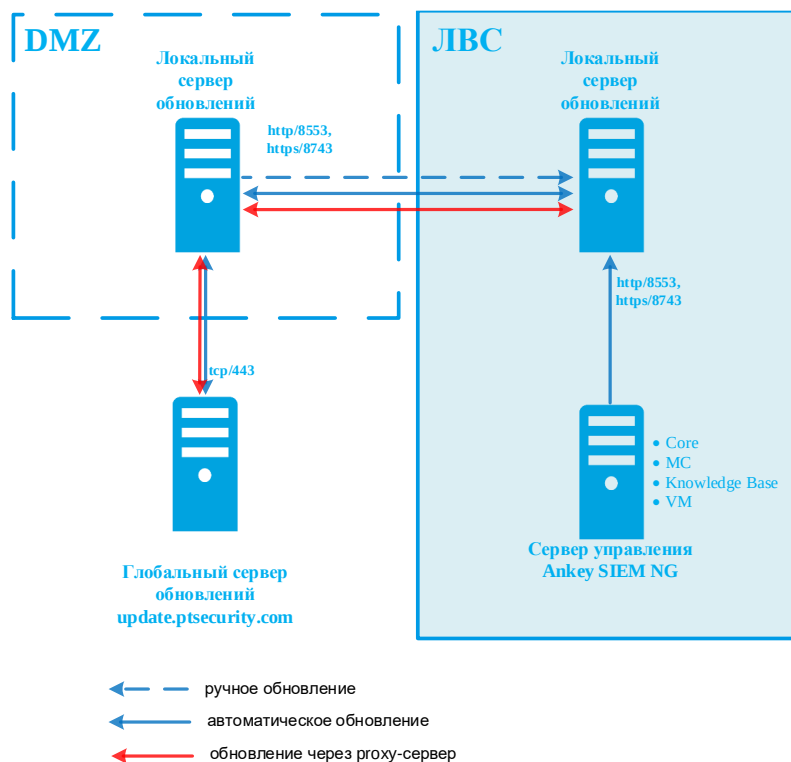


Рисунок 3.27 – Схема получения обновлений с двумя Ankey Update Mirror, установленными в закрытом сегменте сети и в демилитаризованной зоне (вариант 2).

Для получения обновлений необходимо:

- при установке (см. подраздел 3.7.5) или обновлении роли Management and Configuration (см. подраздел 4.1.2.3) указать значения параметров ExpertDataUpdateMethod, PackagesSourceUri и PackagesSourceCredentialToken;
- установить два локальных сервера обновлений: в закрытом сегменте сети и в демилитаризованной зоне;
- если планируется ручной перенос обновлений между локальными серверами в закрытом сегменте сети и демилитаризованной зоне – активировать лицензию на локальном сервере обновлений, установленном в демилитаризованной зоне;
- если планируется автоматический перенос обновлений между локальными серверами в закрытом сегменте сети и демилитаризованной зоне – активировать лицензии обоих локальных серверов обновлений;
- если между локальными серверами обновлений есть сетевое взаимодействие и необходимо автоматизировать процесс обновления – настроить подключение локального сервера обновлений в изолированном сегменте сети к локальному серверу в демилитаризованной зоне.

3.23.2 Удаление компонента UCS

Начиная с версии Ankey SIEM NG 5.2.3 функцию доставки экспертных данных выполняет локальный сервер обновлений Ankey Update Mirror.

Если до обновления ПК Ankey SIEM NG с версии 4.x на 5.x для выполнения этой функции был установлен компонент UCS, вы можете удалить его с целью освобождения дискового пространства, поскольку после установки Ankey Update Mirror этот компонент более не потребуется.

Примечание. Удаление компонента UCS требуется только при его наличии.

1. Для удаления пакетов компонента UCS выполните команду:
`apt-get --purge autoremove ucs-ankey ucs-branding`
После выполнения команды отобразятся предупреждения, свидетельствующие о неполном удалении:
`dpkg: предупреждение: при удалении ucs-ankey каталог «/srv/updater/products» не пуст, поэтому не удалён`
`dpkg: предупреждение: при удалении ucs-ankey каталог «/srv/updater/fus» не пуст, поэтому не удалён`
`dpkg: предупреждение: при удалении ucs-ankey каталог «/srv/salt» не пуст, поэтому не удалён`
`dpkg: предупреждение: при удалении ucs-ankey каталог «/opt/ucs/ucs-ankey/salt» не пуст, поэтому не удалён`
`dpkg: предупреждение: при удалении ucs-ankey каталог «/etc/opt/ucs/ucs-ankey» не пуст, поэтому не удалён`
`dpkg: предупреждение: при удалении ucs-branding каталог «/opt/siem/ucs-branding/salt» не пуст, поэтому не удалён`
2. Для полной очистки необходимо удалить каталоги UCS:
`rm -R /srv/updater/`
`rm -R /srv/salt/`
`rm -R /opt/ucs/`
`rm -R /opt/siem/ucs-branding/`
`rm -R /etc/opt/ucs/`

3.23.3 Изменение параметров обновления экспертных данных для роли Management and Configuration

Перед настройкой подключения к серверу обновлений нужно получить токен для аутентификации и настроить параметры обновления экспертных данных для роли Management and Configuration. Новые пользователи Ankey SIEM NG получают токен вместе с лицензией на продукт. Токен хранится в файле `instance-access-token.key` и представляет собой набор символов, закодированных с использованием стандарта Base64. Этот набор символов необходимо будет указать в качестве значения конфигурационного параметра `PackagesSourceCredentialToken` на одном из шагов инструкции.

Примечание. Чтобы получить новый токен аутентификации, необходимо обратиться в техническую поддержку ООО «Газинформсервис».

Чтобы изменить параметры роли:

1. На сервере с установленной ролью **Deployer** распакуйте архив `managementandconfiguration_<Номер версии>.tar.gz` из комплекта поставки:
`tar -xvf managementandconfiguration_<Номер версии>.tar.gz`
2. Запустите сценарий:
`managementandconfiguration_<Номер версии>/install.sh`
3. В открывшемся окне нажмите кнопку **Yes**.
4. В открывшемся окне выберите вариант с идентификатором приложения роли.
5. В открывшемся окне выберите вариант с названием экземпляра роли.
Откроется окно для выбора набора параметров.
6. Выберите вариант **Advanced configuration**.
7. Откроется страница со списком параметров (см. приложение Б).
8. В качестве значения параметра `ExpertDataUpdateMethod` выберите:
 - если обновление экспертных данных будет осуществляться напрямую с сервера обновлений «Газинформсервис» или с помощью локального сервера обновлений – **Online**;
 - если вручную – **Offline**.
9. В качестве значения параметра `PackagesSourceUri` укажите:
 - если Ankey SIEM NG установлен в сегменте сети с прямым подключением к интернету – адрес глобального сервера обновлений `https://update.ptsecurity.com/packman/v1/`.
 - если в изолированном сегменте сети без прямого подключения к интернету – адрес локального сервера обновлений в формате `http://<Адрес сервера>:<Порт>/packman/v1/`.

Примечание. Указанный в параметре порт локального сервера обновлений должен быть открыт для входящих соединений. Для подключения по протоколам HTTP и HTTPS по умолчанию используются порты 8553 и 8743 соответственно.

10. В качестве значения параметра `PackagesSourceCredentialToken` укажите содержимое файла `instance-access-token.key`.

Примечание. Для вставки содержимого файла в поле параметра `PackagesSourceCredentialToken` можно использовать сочетание клавиш **Shift+Insert**.

11. Нажмите кнопку **OK**.
Начнется изменение конфигурации роли. По его завершении появится сообщение `Deployment configuration successfully applied`.
12. Нажмите кнопку **OK**.
Параметры роли изменены.

3.23.4 Аппаратные и программные требования к локальному серверу обновлений

Локальный сервер обновлений может быть установлен как на физическом сервере, так или в виртуальной среде.

Примечание. Вы можете установить локальный сервер обновлений на один сервер с ролью Deployer.

Аппаратные требования

Для работы сервера требуются следующие минимальные аппаратные ресурсы:

- 1 ядро процессора;
- 2 ГБ оперативной памяти;
- 100 ГБ свободного места на диске.

Программные требования

Локальный сервер обновлений поддерживает установку на операционные системы семейства Linux – Astra Linux Special Edition 1.7, Debian 10, Debian 11, Ubuntu 18.04 или Ubuntu 22.04.

3.23.5 Установка локального сервера обновлений

В разделе приводится инструкция по установке локального сервера обновлений в закрытом сегменте сети или в демилитаризованной зоне.

Примечание. По умолчанию локальный сервер обновлений использует для подключения по протоколам HTTP и HTTPS порты 8553 и 8743 соответственно. Вы можете изменить (см. раздел 3.23.10) эти значения в параметрах сервиса получения обновлений.

Перед выполнением инструкции нужно убедиться, что физический сервер или виртуальная машина, на которые вы планируете устанавливать локальный сервер обновлений, удовлетворяет аппаратным и программным требованиям (см. раздел 3.23.4).

Чтобы установить локальный сервер обновлений:

1. Скопируйте архив с дистрибутивом локального сервера обновлений в любой каталог на сервере или виртуальной машине, на которые планируете устанавливать локальный сервер обновлений.

Примечание. Архив имеет название `ankey-update-mirror-<Версия локального сервера обновлений>.tar.gz` и содержит установочный пакет `ankey-update-mirror-<Версия локального сервера обновлений>.deb`, исполняемый файл `ankey-update-mirror`, конфигурационный файл `config.json` и информационный файл `README.md`.

2. Перейдите в каталог со скопированным архивом:

- cd <Путь к каталогу с архивом>
3. **Распакуйте скопированный архив:**
`tar -xvf ankey-update-mirror-<Версия локального сервера обновлений>.tar.gz`
 4. **Запустите установку локального сервера обновлений:**
`dpkg -i ankey-update-mirror-<Версия локального сервера обновлений>.deb`
Локальный сервер обновлений установлен.
При установке локального сервера обновлений создается пользователь `ankey-update-mirror`, который используется при выполнении сервером различных операций.

Если локальный сервер обновлений установлен в демилитаризованной зоне, необходимо активировать на нем лицензию в соответствии с инструкцией (см. раздел 3.23.6).

Если локальный сервер обновлений установлен в закрытом сегменте сети, активировать на нем лицензию необходимо только в случае, когда планируется автоматический перенос обновлений (см. раздел 3.22.6) между локальными серверами в закрытом сегменте сети и демилитаризованной зоне.

3.23.6 Активация лицензии локального сервера обновлений

После установки локального сервера обновлений нужно активировать его лицензию. Это необходимо для аутентификации локального сервера на глобальном сервере обновлений «Газинформсервис».

Примечание. Если перенос обновлений на локальный сервер будет осуществляться вручную, активировать его лицензию не нужно.

Вы можете активировать лицензию с помощью токена лицензии, который хранится в файле `license-access-token.key`, полученном на физическом носителе или в электронном письме на адрес, указанный при покупке.

Примечание. При наличии нескольких лицензий вы можете активировать их по очереди.

Если локальный сервер обновлений должен подключаться к интернету через прокси-сервер, перед активацией лицензии нужно настроить подключение к этому прокси-серверу.

Активация лицензии с помощью токена лицензии

Чтобы активировать лицензию с помощью токена лицензии:

1. **Выполните команду:**
`sudo /opt/ankey/ankey-update-mirror/bin/ankey-update-mirror license activate --license-token <Путь к файлу license-access-token.key>`
2. **Запустите процесс скачивания обновлений с помощью команды обновления репозитория:**
`sudo /opt/ankey/ankey-update-mirror/bin/ankey-update-mirror repository update`

Лицензия активирована.

3.23.7 Настройка подключения локального сервера обновлений к прокси-серверу

Для подключения локального сервера обновлений к интернету через прокси-сервер необходимо указать параметры этого подключения в конфигурационном файле локального сервера.

Локальный сервер обновлений поддерживает подключение к прокси-серверу по протоколам HTTP и HTTPS.

Подключение к прокси-серверу по протоколу HTTP

Чтобы настроить подключение локального сервера обновлений к прокси-серверу:

1. На локальном сервере обновлений откройте конфигурационный файл `config.json`:
`sudo nano /etc/ankey-update-mirror/config.json`
2. В качестве значения параметра `proxy` укажите IP-адрес (и при необходимости порт) используемого прокси-сервера:
`"proxy": "http://<IP-адрес прокси-сервера>:<Порт>"`
3. Если прокси-сервер требует аутентификации, укажите логин и пароль для подключения:
`"proxy-user": "<Логин>",`
`"proxy-password": "<Пароль>"`
4. Сохраните изменения в файле `config.json`.
5. Перезапустите локальный сервер обновлений:
`sudo systemctl restart ankey-update-mirror.service`

Подключение настроено.

Подключение к прокси-серверу по протоколу HTTPS

Для проверки подлинности при передаче данных по протоколу HTTPS необходимо выпустить сертификат SSL, который должен:

- соответствовать формату PEM;
- использовать подпись с применением алгоритма шифрования SHA-256;
- использовать алгоритм шифрования ключей RSA;
- содержать закрытый незашифрованный ключ в формате PEM длиной не менее 2048 бит;
- включать в себя область применения сертификата Digital Signature или Key Encipherment;
- содержать в расширении Subject Alternative Name (SAN) запись о доменном имени или IP-адресе сервера с установленным веб-интерфейсом продукта;
- если в цепочке между корневым сертификатом и сертификатами компонентов и систем есть промежуточные сертификаты – включать в себя всю цепочку сертификатов.

Для корректной работы необходимо добавить выпущенный сертификат в список доверенных.

Чтобы добавить сертификат в список доверенных:

1. Скопируйте файлы сертификата в каталог `/usr/local/share/ca-certificates/` на узле, на который установлен локальный сервер обновлений.

2. Обновите список доверенных сертификатов:

```
sudo update-ca-certificates
```

Сертификат добавлен в список доверенных.

❖ Чтобы настроить подключение локального сервера обновлений к прокси-серверу:

1. На локальном сервере обновлений откройте конфигурационный файл config.json:

```
sudo nano /etc/ankey-update-mirror/config.json
```
2. В качестве значения параметра proxy укажите IP-адрес (и при необходимости порт) используемого прокси-сервера:

```
"proxy": "https://<IP-адрес прокси-сервера>:<Порт>"
```
3. Если прокси-сервер требует аутентификации, укажите логин и пароль для подключения:

```
"proxy-user": "<Логин>",  
"proxy-password": "<Пароль>"
```
4. Сохраните изменения в файле config.json.
5. Перезапустите локальный сервер обновлений:

```
sudo systemctl restart ankey-update-mirror.service
```

Подключение настроено.

3.23.8 Настройка автоматического переноса обновлений в закрытый сегмент сети

Если между локальными серверами обновлений есть сетевое взаимодействие, вы можете настроить их подключение друг к другу. Это позволит автоматически переносить обновления с глобального сервера обновлений «Газинформсервис» в Ankey SIEM NG в закрытом сегменте сети через цепочку локальных серверов обновлений.

Вы можете настроить автоматический перенос обновлений как по протоколу HTTP, так и по протоколу HTTPS.

Подключение по протоколу HTTP

Для подключения по протоколу HTTP вместо порта по умолчанию 80 используется порт 8553. Если требуется, вы можете изменить порт (см. раздел 3.23.10) для подключения.

Чтобы настроить автоматический перенос обновлений:

1. На локальном сервере обновлений в изолированном сегменте откройте конфигурационный файл config.json:

```
sudo nano /etc/ankey-update-mirror/config.json
```
2. В качестве значения параметра update-server укажите адрес локального сервера обновлений в демилитаризованной зоне:

```
"update-server": "http://<Адрес локального сервера обновлений>:<Порт>"
```

Примечание. Указанный в параметре порт локального сервера обновлений должен быть открыт для входящих соединений.

3. В качестве значения параметра verify_ssl укажите false.

4. Если подключение к локальному серверу в демилитаризованной зоне выполняется через прокси-сервер, настройте параметры подключения к прокси-серверу (см. раздел 3.23.7).
5. Сохраните изменения в файле `config.json`.
6. Перезапустите сервис обновлений в закрытом сегменте сети:
`sudo systemctl restart ankey-update-mirror.service`

Перенос обновлений настроен.

Подключение по протоколу HTTPS

Для подключения по протоколу HTTPS вместо порта по умолчанию 443 используется порт 8743. Если требуется, вы можете изменить порт (см. раздел 3.23.10) для подключения.

Для проверки подлинности при передаче данных по протоколу HTTPS необходимо выпустить сертификат SSL, который должен:

- соответствовать формату PEM;
- использовать подпись с применением алгоритма шифрования SHA-256;
- использовать алгоритм шифрования ключей RSA;
- содержать закрытый незашифрованный ключ в формате PEM длиной не менее 2048 бит;
- включать в себя область применения сертификата Digital Signature или Key Encipherment;
- содержать в расширении Subject Alternative Name (SAN) запись о доменном имени или IP-адресе сервера с установленным веб-интерфейсом продукта;
- если в цепочке между корневым сертификатом и сертификатами компонентов и систем есть промежуточные сертификаты – включать в себя всю цепочку сертификатов.

Для корректной работы необходимо назвать файлы сертификата и его ключа `cert.crt` и `cert.key` соответственно и поместить их в каталог `/etc/ankey-update-mirror/https_certs/` на локальном сервере обновлений.

Чтобы настроить автоматический перенос обновлений:

1. На локальном сервере обновлений в изолированном сегменте откройте конфигурационный файл `config.json`:
`sudo nano /etc/ankey-update-mirror/config.json`
2. В качестве значения параметра `update-server` укажите адрес локального сервера обновлений в демилитаризованной зоне:
`"update-server": "https://<Адрес локального сервера обновлений>:<Порт>"`

Примечание. Указанный в параметре порт локального сервера обновлений должен быть открыт для входящих соединений.

3. Если подключение к локальному серверу в демилитаризованной зоне выполняется через прокси-сервер, настройте параметры подключения к прокси-серверу (см. раздел 3.23.7).
4. Сохраните изменения в файле `config.json`.
5. Перезапустите сервис обновлений в закрытом сегменте сети:
`sudo systemctl restart ankey-update-mirror.service`

Перенос обновлений настроен.

3.23.9 Ручной перенос обновлений Ankey SIEM NG в закрытый сегмент сети

Если между локальными серверами обновлений отсутствует сетевое взаимодействие, вам нужно вручную перенести обновления в закрытый сегмент сети для последующего обновления Ankey SIEM NG.

Чтобы вручную перенести обновления в закрытый сегмент сети:

1. На локальном сервере обновлений в демилитаризованной зоне запустите получение обновлений с глобального сервера обновлений «Газинформсервис»:

```
sudo /opt/ankey/ankey-update-mirror/bin/ankey-update-mirror repository update
```
2. Запустите экспорт репозитория с обновлениями в файл:

```
sudo /opt/ankey/ankey-update-mirror/bin/ankey-update-mirror repository export --repo vm-expertise <Название файла>.tgz
```

Примечание. Выполнение команды экспорта без ключа `--repo <Название репозитория>` позволяет экспортировать все репозитории базы обновлений в указанный архив. Вы можете просмотреть список репозиторий в базе обновлений локального сервера с помощью команды `sudo /opt/ankey/ankey-update-mirror/bin/ankey-update-mirror repository view`.

3. Скопируйте с помощью внешнего носителя полученный файл архива в каталог, принадлежащий пользователю `ankey-update-mirror`, на локальном сервере обновлений в закрытом сегменте сети.
4. На локальном сервере обновлений в закрытом сегменте сети импортируйте обновления из скопированного файла архива:

```
sudo /opt/ankey/ankey-update-mirror/bin/ankey-update-mirror repository import <Путь к архиву>/<Название архива>.tgz
```

Обновления Ankey SIEM NG перенесены.

3.23.10 Проверка и изменение параметров локального сервера обновлений

Проверка состояния сервера

Чтобы проверить состояние локального сервера обновлений, на локальном сервере выполните команду:

```
sudo systemctl status ankey-update-mirror
```

На экране отобразится информация о параметрах загрузки и состоянии локального сервера.

Проверка состояния таймера получения обновлений

Чтобы проверить состояние таймера получения обновлений, на локальном сервере выполните команду:

```
sudo systemctl status ankey-update-mirror-update.timer
```

На экране отобразится информация о параметрах загрузки и состоянии таймера получения обновлений.

Проверка состояния сервиса получения обновлений

Чтобы проверить состояние сервиса получения обновлений,

на локальном сервере выполните команду:

```
sudo systemctl status ankey-update-mirror-update
```

На экране отобразится информация о параметрах загрузки и состоянии сервиса получения обновлений.

Просмотр журналов событий сервиса получения обновлений

Чтобы просмотреть журнал событий сервиса получения обновлений,

на локальном сервере выполните команду:

```
journalctl -u ankey-update-mirror.service
```

На экране отобразится список событий сервиса получения обновлений.

Изменение времени получения обновлений

По умолчанию обновление запускается в 13, 27, 42 и 58 минут каждого часа. Вы можете изменить эти значения в параметрах таймера получения обновлений.

Чтобы изменить время получения обновлений:

1. Откройте файл `ankey-update-mirror-update.timer`:

```
sudo nano /etc/systemd/system/ankey-update-mirror-update.timer
```
2. В блоке параметров `Timer` в качестве значения параметра `OnCalendar` укажите нужное время получения обновлений (в формате `systemd.timer`).
3. Сохраните изменения в файле `ankey-update-mirror-update.timer`.
4. Примените изменения таймера:

```
sudo systemctl daemon-reload
```
5. Перезапустите таймер получения обновлений:

```
sudo systemctl restart ankey-update-mirror-update.timer
```

Время получения обновлений изменено.

Изменение порта подключения по протоколам HTTP и HTTPS

По умолчанию локальный сервер обновлений использует для подключения по протоколам HTTP и HTTPS порты 8553 и 8743 соответственно. Вы можете изменить эти значения в параметрах сервиса получения обновлений.

Чтобы изменить порт подключения:

1. Откройте файл `ankey-update-mirror.service`:

```
sudo nano /etc/systemd/system/ankey-update-mirror.service
```
2. Выполните одно из следующих действий:
 - если для подключения локального сервера используется протокол HTTP, в блок параметров `Service` в конец строки с параметром `ExecStart` добавьте ключ `--http-port <Порт>`.
 - если для подключения локального сервера используется протокол HTTPS, в блок параметров `Service` в конец строки с параметром `ExecStart` добавьте ключ `--https-port <Порт>`.
3. Сохраните изменения в файле `ankey-update-mirror.service`.
4. Примените изменения таймера:

```
sudo systemctl daemon-reload
```
5. Перезапустите локальный сервер обновлений:

```
sudo systemctl restart ankey-update-mirror
```

Порт подключения изменен.

3.24 Настройка ПК Ankey SIEM NG для обеспечения его безопасной работы

В этом подразделе приводятся инструкции по настройке развернутой конфигурации ПК Ankey SIEM NG для обеспечения его безопасной работы.

Компоненты системы рекомендуется разместить в доверенном сегменте сети. Доступ к ним из других сегментов рекомендуется ограничить с помощью межсетевого экрана.

3.24.1 Настройка ПК Ankey SIEM NG в конфигурации для низконагруженных систем

Чтобы настроить ПК Ankey SIEM NG:

1. На серверах под управлением Linux разрешите удаленный доступ по протоколу SSH только с рабочих станций администраторов:

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT  
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций администраторов> -p tcp -m tcp --dport 22 -m conntrack --ctstate NEW -m comment --comment "SSH admin access" -j ACCEPT
```

Примечание. IP-адреса рабочих станций необходимо перечислять через запятую. Также вы можете указать маску подсети, где находятся рабочие станции, в формате CIDR. Например, -s 198.51.100.0,198.51.100.1,192.0.2.0/24.

2. На сервере Ankey SIEM NG Core разрешите доступ к веб-интерфейсу системы с рабочих станций пользователей:

```
iptables -F DOCKER-USER  
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT  
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций пользователей> -p tcp -m multiport --dports 443,3334,8091,8190 -m conntrack --ctstate NEW -m comment --comment "Web user access" -j ACCEPT
```

Примечание. Служба PgAdmin не устанавливается вместе с СУБД Jatoba по умолчанию. Если вы используете СУБД Jatoba, перейдите к п. 7.

3. В файл `custom.env`, расположенный в каталоге `/var/lib/deployed roles/<Идентификатор приложения Ankey SIEM NG>/<Название экземпляра роли SqlStorage>/images/storage-pgadmin/config/`, добавьте параметры:

```
PGADMIN_CONFIG_MASTER_PASSWORD_REQUIRED=True  
PGADMIN_DEFAULT_PASSWORD=<Пароль PGAdmin>
```

4. **Перезапустите службы компонентов Ankey SIEM NG Core и Knowledge Base:**
`docker restart $(docker ps | awk '/core-[kb-/{print $NF}')`
5. **Пересоберите службу pgAdmin:**
`cd /var/lib/deployed-roles/<Идентификатор приложения Management and Configuration>/<Название экземпляра роли SqlStorage>/images/storage-pgadmin`
`docker-compose down`
`docker-compose up -d`
6. **Разрешите доступ к панели управления pgAdmin с рабочих станций администраторов:**
`iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций администраторов> -p tcp -m conntrack --ctstate NEW --ctorigdstport 9001 -m comment --comment "pgAdmin access" -j ACCEPT`
7. **Разрешите входящие соединения от коллекторов:**
`iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG Collector> -p tcp -m tcp --dport 5671 -m conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG Collector to Ankey SIEM NG Server" -j ACCEPT`
8. **Разрешите входящие соединения от Ankey SIEM NG RC:**
`iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG RC> -p tcp -m multiport --dports 443,3334,5671,8091 -m conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG RC to Ankey SIEM NG Core" -j ACCEPT`
`iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG RC> -p tcp -m tcp --dport 8013 -m conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG RC to Ankey SIEM NG Server" -j ACCEPT`
9. **На серверах под управлением Linux заблокируйте все входящие соединения, кроме разрешенных:**
`iptables -A INPUT -i <Название внешнего сетевого интерфейса> -j DROP`
`iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -j REJECT`
10. **Для сохранения созданных правил на серверах под управлением Debian установите пакет iptables-persistent:** `apt-get install iptables-persistent`

Примечание. Порядок сохранения правил на серверах под управлением Astra Linux описан в [справочном центре производителя операционной системы](#).

11. **Сохраните правила межсетевого экрана:** `netfilter-persistent save`
12. **На серверах коллекторов под управлением Windows Server удалите все правила удаленного доступа по протоколу RDP:**
`netsh advfirewall firewall delete rule name=all protocol=tcp localport=3389`

```
netsh advfirewall firewall delete rule name=all protocol=udp
localport=3389
```

13. **Разрешите удаленный доступ по протоколу RDP только с рабочих станций администраторов:**

```
netsh advfirewall firewall add rule name="Allow RDP TCP in" dir=in
action=allow
protocol=tcp localport=3389 remoteip=<IP-адреса рабочих станций
администраторов>
netsh advfirewall firewall add rule name="Allow RDP UDP in" dir=in
action=allow
protocol=udp localport=3389 remoteip=<IP-адреса рабочих станций
администраторов>
```

Примечание. IP-адреса рабочих станций необходимо перечислять через запятую. Также вы можете указать маску подсети, где находятся рабочие станции, в формате CIDR. Например, remoteip=198.51.100.0,198.51.100.1,192.0.2.0/24.

14. Если для сбора событий по стандарту syslog и протоколу Netflow коллекторы на Windows Server не используют порты по умолчанию, на серверах коллекторов удалите правила для входящих соединений с этих портов:

```
for %P IN (514,1468) DO (netsh advfirewall firewall delete rule name=all
protocol=tcp localport=%P)
for %P IN (514,2055) DO (netsh advfirewall firewall delete rule name=all
protocol=udp localport=%P)
```

15. Разрешите входящие соединения для сбора событий по стандарту syslog и протоколу Netflow на серверах коллекторов на Linux для портов, указанных при создании задачи на сбор событий:

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -p tcp -m
tcp --dport 1468 -m conntrack --ctstate NEW -m comment --comment
"Agent SysLog (TCP)" -j ACCEPT
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -p udp -
m udp --dport 514 -m conntrack --ctstate NEW -m comment --comment
"Agent SysLog (UDP)" -j ACCEPT
```

16. Смените пароли служебных учетных записей в ПК Ankey SIEM NG (подробнее см. Руководство администратора Ankey SIEM NG 5.2.3).

17. На серверах под управлением Windows Server убедитесь, что пароли для входа в операционную систему соответствуют требованиям к сложности, установленным в организации.

18. Установите собственные доверенные сертификаты (см. подраздел 3.21) для Ankey SIEM NG Core, Knowledge Base, Ankey SIEM NG MC и RabbitMQ.

19. На серверах под управлением Linux для каждого администратора ПК Ankey SIEM NG создайте отдельную учетную запись:

```
adduser <Логин администратора>
```

20. На рабочих станциях администраторов ПК Ankey SIEM NG настройте подключение по протоколу SSH с помощью ключей:

- сгенерируйте ключевую пару с помощью утилиты `ssh-keygen`, например:

```
ssh-keygen -o -a 100 -t ed25519 -f ~/.ssh/siem
```

где:

`o` – указание сохранить приватный ключ с использованием формата OpenSSH вместо PEM;

`a` – указание количества циклов KDF (Key Derivation Function, функция формирования ключа);

Высокие значения приведут к замедлению проверки парольной фразы, увеличивая её устойчивость к перебору при краже приватного ключа;

`t` – указание типа создаваемого ключа, например, с использованием алгоритма `ed25519`;

Внимание! Перед созданием ключевой пары убедитесь в том, что вы не используете название и путь, которые дублируют уже существующую пару ключей. Это позволит избежать случайной потери данных.

- введите и подтвердите пароль для ключевой пары;
- нажмите **Enter**, чтобы принять все внесенные изменения.

```
gis@core:~$ ssh-keygen -o -a 100 -t ed25519 -f ~/.ssh/siem
Generating public/private ed25519 key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/gis/.ssh/siem
Your public key has been saved in /home/gis/.ssh/siem.pub
The key fingerprint is:
SHA256:TNoLx3IPT7Cz... gis@core
The key's randomart image is:
+--[ED25519 256]--+
|
|
|
|
|
|
+-----[SHA256]-----+
```

Рисунок 3.28 – Пример генерации пары ключей

- передайте открытый ключ с расширением `.pub` на удаленные серверы под управлением Linux, с которыми необходимо установить соединение:

```
ssh-copy-id -i <путь до открытого ключа>/<название открытого ключа>.pub <Логин администратора>@<адрес удаленного сервера>
```

Открытый ключ будет сохранен по пути

/home/<Логин администратора>/.ssh/authorized_keys

- на каждом удаленном сервере в файле /etc/ssh/sshd_config раскомментируйте и измените значения параметров (разрешите вход только с помощью SSH-ключей):

PubkeyAuthentication yes

RhostsRSAAuthentication no

HostbasedAuthentication no

PermitEmptyPasswords no

PasswordAuthentication no

- на каждом удаленном сервере в файле /etc/sudoers измените значение параметра:

<Логин администратора> ALL=(ALL) ALL

21. Для каждого пользователя ПК Ankey SIEM NG создайте отдельную учетную запись.

22. Смените пароль учетной записи Administrator

ПК Ankey SIEM NG настроен.

3.24.2 Настройка ПК Ankey SIEM NG в конфигурации для средненагруженных систем

Чтобы настроить ПК Ankey SIEM NG:

1. На серверах под управлением Linux разрешите удаленный доступ по протоколу SSH только с рабочих станций администраторов:

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -m  
conntrack --ctstate
```

```
ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-  
адреса рабочих станций администраторов> -p tcp -m tcp --dport 22 -m  
conntrack --ctstate NEW -m comment --comment "SSH admin access" -j  
ACCEPT
```

Примечание. IP-адреса рабочих станций необходимо перечислять через запятую. Также вы можете указать маску подсети, где находятся рабочие станции, в формате CIDR. Например, -s 198.51.100.0,198.51.100.1,192.0.2.0/24.

2. На сервере Ankey SIEM NG Core разрешите доступ к веб-интерфейсу системы с рабочих станций пользователей:

```
iptables -F DOCKER-USER
```

```
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса>  
-m conntrack --ctstate
```

```
ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса>  
-s <IP-адреса рабочих станций пользователей> -p tcp -m multiport --  
dports 443,3334,8091,8190 -m conntrack --ctstate NEW -m comment --  
comment "Web user access" -j ACCEPT
```

3. На сервере с установленной ролью Deployer разрешите входящие соединения от сервера Ankey SIEM NG Server:

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG Server> -p tcp -m multiport --dports 4505,4506 -m conntrack --ctstate NEW -m comment --comment "From MP Siem Server to Deployer" -j ACCEPT
```

```
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG Server> -p tcp --dport 5000 -m conntrack --ctstate NEW -m comment --comment "From MP Siem Server to Deployer" -j ACCEPT
```

Примечание. Служба PgAdmin не устанавливается вместе с СУБД Jatoba по умолчанию. Если вы используете СУБД Jatoba, перейдите к п. 7.

4. В файл custom.env, расположенный в каталоге /var/lib/deployed roles/<Идентификатор приложения Ankey SIEM NG>/<Название экземпляра роли SqlStorage/JatobaStorage>/images/storage-pgadmin/config/, добавьте параметры:
PGADMIN_CONFIG_MASTER_PASSWORD_REQUIRED=True
PGADMIN_DEFAULT_PASSWORD=<Пароль PGAdmin>
5. Пересоберите службу pgAdmin:
cd /var/lib/deployed-roles/<Идентификатор приложения Management and Configuration>/<Название экземпляра роли SqlStorage>/images/storage-pgadmin
docker-compose down
docker-compose up -d
6. Разрешите доступ к панели управления pgAdmin с рабочих станций администраторов:
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций администраторов> -p tcp -m conntrack --ctstate NEW --ctorigdstport 9001 -m comment --comment "pgAdmin access" -j ACCEPT
7. Разрешите входящие соединения от Ankey SIEM NG Server:
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG Server> -p tcp -m multiport --dports 443,3334,5671,8703,8721,8799 -m conntrack -ctstate NEW -m comment --comment "From Ankey SIEM NG Server to Ankey SIEM NG Core" -j ACCEPT
8. Разрешите входящие соединения от Ankey SIEM NG RC:
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG RC> -p tcp -m multiport --dports 443,3334,5671,8091 -m conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG RC to Ankey SIEM NG Core" -j ACCEPT
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG RC> -p tcp -m tcp --dport 8013 -m conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG RC to Ankey SIEM NG Server" -j ACCEPT
На сервере Ankey SIEM NG Server разрешите входящие соединения от Ankey SIEM NG Core:

```
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса>
-s <IP-адрес сервера Ankey SIEM NG Core> -p tcp -m tcp --dport 8013 -m
conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG
Core to Ankey SIEM NG Server" -j ACCEPT
```

```
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса>
-s <IP-адрес сервера Ankey SIEM NG Core> -p tcp -m multiport --dports
5671,5672,15672 -m conntrack --ctstate NEW -m comment --comment
"From Ankey SIEM NG Core to Ankey SIEM NG Server" -j ACCEPT
```

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-
адрес сервера Ankey SIEM NG Core> -p tcp --dport 9200 -m conntrack --
ctstate NEW -m comment --comment "From Ankey SIEM NG Core to Ankey
SIEM NG Events Storage" -j ACCEPT
```

9. **Если в качестве хранилища событий используется Elasticsearch:**

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-
адрес сервера Ankey SIEM NG Core> -p tcp --dport 9200 -m conntrack --
ctstate NEW -m comment --comment "From Ankey SIEM NG Core to Ankey
SIEM NG Events Storage" -j ACCEPT
```

10. **Если в качестве хранилища событий используется LogSpace:**

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-
адрес сервера Ankey SIEM NG Core> -p tcp --dport 8123 -m conntrack --
ctstate NEW -m comment --comment "From Ankey SIEM NG Core to Ankey
SIEM NG Events Storage" -j ACCEPT
```

11. **Разрешите входящие соединения от Ankey SIEM NG RC:**

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-
адрес сервера Ankey SIEM NG RC> -p tcp -m tcp --dport 8013 -m conntrack
--ctstate NEW -m comment --comment "From Ankey SIEM NG RC to Ankey
SIEM NG Server" -j ACCEPT
```

12. **На серверах под управлением Linux заблокируйте все входящие соединения, кроме разрешенных:**

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -j DROP
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса>
-j REJECT
```

13. **Для сохранения созданных правил на серверах под управлением Debian установите пакет iptables-persistent: apt-get install iptables-persistent**

Примечание. Порядок сохранения правил на серверах под управлением Astra Linux описан в [справочном центре производителя операционной системы](#).

14. **Сохраните правила межсетевого экрана: netfilter-persistent save**

15. **На серверах коллекторов под управлением Windows Server удалите все правила удаленного доступа по протоколу RDP:**

```
netsh advfirewall firewall delete rule name=all protocol=tcp
localport=3389
netsh advfirewall firewall delete rule name=all protocol=udp
localport=3389
```

16. Разрешите удаленный доступ по протоколу RDP только с рабочих станций администраторов:

```
netsh advfirewall firewall add rule name="Allow RDP TCP in" dir=in
action=allow
protocol=tcp localport=3389 remoteip=<IP-адреса рабочих станций
администраторов>
netsh advfirewall firewall add rule name="Allow RDP UDP in" dir=in
action=allow
protocol=udp localport=3389 remoteip=<IP-адреса рабочих станций
администраторов>
```

Примечание. IP-адреса рабочих станций необходимо перечислять через запятую. Также вы можете указать маску подсети, где находятся рабочие станции, в формате CIDR. Например, remoteip=198.51.100.0,198.51.100.1,192.0.2.0/24.

17. Если для сбора событий по стандарту syslog и протоколу Netflow коллекторы на Windows Server не используют порты по умолчанию, на серверах коллекторов удалите правила для входящих соединений с этих портов:

```
for %P IN (514,1468) DO (netsh advfirewall firewall delete rule name=all
protocol=tcp localport=%P)
for %P IN (514,2055) DO (netsh advfirewall firewall delete rule name=all
protocol=udp localport=%P)
```

18. Смените пароли служебных учетных записей в ПК Ankey SIEM NG (подробнее см. Руководство администратора Ankey SIEM NG 5.2.3).

19. Разрешите входящие соединения для сбора событий по стандарту syslog и протоколу Netflow на серверах коллекторов на Linux для портов, указанных при создании задачи на сбор событий:

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -p tcp -m
tcp --dport 1468 -m conntrack --ctstate NEW -m comment --comment
"Agent SysLog (TCP)" -j ACCEPT
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -p udp -
m udp --dport 514 -m conntrack --ctstate NEW -m comment --comment
"Agent SysLog (UDP)" -j ACCEPT
```

20. На серверах под управлением Windows Server убедитесь, что пароли для входа в операционную систему соответствуют требованиям к сложности, установленным в организации.

21. Установите собственные доверенные сертификаты (см. подраздел 3.21) для Ankey SIEM NG Core, Knowledge Base, Ankey SIEM NG MC и RabbitMQ.

22. На серверах под управлением Linux для каждого администратора ПК Ankey SIEM NG создайте отдельную учетную запись:

```
adduser <Логин администратора>
```

23. На рабочих станциях администраторов ПК Ankey SIEM NG настройте подключение по протоколу SSH с помощью ключей:

- сгенерируйте ключевую пару с помощью утилиты ssh-keygen, например:
ssh-keygen -o -a 100 -t ed25519 -f ~/.ssh/siem
где:
o – указание сохранить приватный ключ с использованием формата OpenSSH вместо PEM;
a – указание количества циклов KDF (Key Derivation Function, функция формирования ключа);
Высокие значения приведут к замедлению проверки парольной фразы, увеличивая её устойчивость к перебору при краже приватного ключа;
t – указание типа создаваемого ключа, например, с использованием алгоритма ed25519;

Внимание! Перед созданием ключевой пары убедитесь в том, что вы не используете название и путь, которые дублируют уже существующую пару ключей. Это позволит избежать случайной потери данных.

- введите и подтвердите пароль для ключевой пары;
- нажмите **Enter**, чтобы принять все внесенные изменения.

```
gis@core:~$ ssh-keygen -o -a 100 -t ed25519 -f ~/.ssh/siem
Generating public/private ed25519 key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/gis/.ssh/siem
Your public key has been saved in /home/gis/.ssh/siem.pub
The key fingerprint is:
SHA256:TN0Lx3IPT7Cz  gis@core
The key's randomart image is:
+--[ED25519 256]--+
|
|
|
|
|
|
|
|
|
|
+-----[SHA256]-----+
```

Рисунок 3.29 – Пример генерации пары ключей

- передайте открытый ключ с расширением .pub на удаленные серверы под управлением Linux, с которыми необходимо установить соединение:
ssh-copy-id -i <путь до открытого ключа>/<название открытого ключа>.pub <Логин администратора>@<адрес удаленного сервера>
Открытый ключ будет сохранен по пути
/home/<Логин администратора>/.ssh/authorized_keys

- на каждом удаленном сервере в файле `/etc/ssh/sshd_config` раскомментируйте и измените значения параметров (разрешите вход только с помощью SSH-ключей):
`PubkeyAuthentication yes`
`RhostsRSAAuthentication no`
`HostbasedAuthentication no`
`PermitEmptyPasswords no`
`PasswordAuthentication no`
 - на каждом удаленном сервере в файле `/etc/sudoers` измените значение параметра:
`<Логин администратора> ALL=(ALL) ALL`
24. Для каждого пользователя ПК Ankey SIEM NG создайте отдельную учетную запись.
25. Смените пароль учетной записи Administrator33.
- ПК Ankey SIEM NG настроен.

3.24.3 Настройка ПК Ankey SIEM NG в конфигурации для высоконагруженных систем

Чтобы настроить ПК Ankey SIEM NG:

1. На серверах под управлением Linux разрешите удаленный доступ по протоколу SSH только с рабочих станций администраторов:
`iptables -A INPUT -i <Название внешнего сетевого интерфейса> -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT`
`iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций администраторов> -p tcp -m tcp --dport 22 -m conntrack --ctstate NEW -m comment --comment "SSH admin access" -j ACCEPT`
2. На сервере Ankey SIEM NG Core разрешите доступ к веб-интерфейсу системы с рабочих станций пользователей:
`iptables -F DOCKER-USER`
`iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT`
`iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций пользователей> -p tcp -m multiport --dports 443,3334,8091,8190 -m conntrack --ctstate NEW -m comment --comment "Web user access" -j ACCEPT`
3. На сервере с установленной ролью Deployer разрешите входящие соединения от серверов Ankey SIEM NG Server и Ankey SIEM NG Events Storage:
`iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-адреса серверов Ankey SIEM NG Server и Ankey SIEM NG Events Storage> -p tcp -m multiport --dports 4505,4506 -m conntrack --ctstate NEW -m comment --comment "From MP Siem Server to Deployer" -j ACCEPT`

```
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса>  
-s <IP-адреса серверов Ankey SIEM NG Server и Ankey SIEM NG Events  
Storage> -p tcp --dport 5000 -m conntrack --ctstate NEW -m comment --  
comment "From MP Siem Server to Deployer" -j ACCEPT
```

Примечание. Служба PgAdmin не устанавливается вместе с СУБД Jatoba по умолчанию. Если вы используете СУБД Jatoba, перейдите к п. 7.

4. В файл `custom.env`, расположенный в каталоге `/var/lib/deployed roles/<Идентификатор приложения Ankey SIEM NG>/<Название экземпляра роли SqlStorage >/images/storage-pgadmin/config/`, добавьте параметры:
`PGADMIN_CONFIG_MASTER_PASSWORD_REQUIRED=True`
`PGADMIN_DEFAULT_PASSWORD=<Пароль PGAdmin>`
 5. Пересоберите службу `pgAdmin`:
`cd /var/lib/deployed-roles/<Идентификатор приложения Management and Configuration>/<Название экземпляра роли SqlStorage >/images/storage-pgadmin`
`docker-compose down`
`docker-compose up -d`
 6. Разрешите доступ к панели управления `pgAdmin` с рабочих станций администраторов:
`iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса>`
`-s <IP-адреса рабочих станций администраторов> -p tcp -m conntrack --`
`ctstate NEW --ctorigdstport 9001 -m comment --comment "pgAdmin`
`access" -j ACCEPT`
 7. Разрешите входящие соединения от `Ankey SIEM NG Server`:
`iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса>`
`-s <IP-адрес сервера Ankey SIEM NG Server> -p tcp -m multiport --dports`
`443,3334,5671,8703,8721,8799 -m conntrack -ctstate NEW -m comment --`
`comment "From Ankey SIEM NG Server to Ankey SIEM NG Core" -j ACCEPT`
 8. Разрешите входящие соединения от `Ankey SIEM NG RC`:
`iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса>`
`-s <IP-адрес сервера Ankey SIEM NG RC> -p tcp -m multiport --dports`
`443,3334,5671,8091 -m conntrack --ctstate NEW -m comment --comment`
`"From Ankey SIEM NG RC to Ankey SIEM NG Core" -j ACCEPT`
- ```
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса>
-s <IP-адрес сервера Ankey SIEM NG RC> -p tcp -m tcp --dport 8013 -m
conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG
RC to Ankey SIEM NG Server" -j ACCEPT
```
9. На сервере `Ankey SIEM NG Server` разрешите входящие соединения от `Ankey SIEM NG Core`:  
`iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса>`  
`-s <IP-адрес сервера Ankey SIEM NG Core> -p tcp -m tcp --dport 8013 -m`

```
conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG
Core to Ankey SIEM NG Server" -j ACCEPT
```

```
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса>
-s <IP-адрес сервера Ankey SIEM NG Core> -p tcp -m multiport --dports
5671,5672,15672 -m conntrack --ctstate NEW -m comment --comment
"From Ankey SIEM NG Core to Ankey SIEM NG Server" -j ACCEPT
```

**10. Разрешите входящие соединения от коллекторов:**

```
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса>
-s <IP-адрес сервера Ankey SIEM NG Collector> -p tcp -m tcp --dport 5671
-m conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG
Collector to Ankey SIEM NG Server" -j ACCEPT
```

**11. На сервере Ankey SIEM NG Events Storage разрешите входящие  
соединения от Ankey SIEM NG Core и Ankey SIEM NG Server:**

- Если в качестве хранилища событий используется  
Elasticsearch:

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -
s <IP-адрес сервера Ankey SIEM NG Server> -p tcp --dport 9200 -m
conntrack --ctstate NEW -m comment --comment "From Ankey
SIEM NG Server to Ankey SIEM NG Events Storage" -j ACCEPT
```

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -
s <IP-адрес сервера Ankey SIEM NG Core> -p tcp --dport 9200 -m
conntrack --ctstate NEW -m comment --comment "From Ankey
SIEM NG Core to Ankey SIEM NG Events Storage" -j ACCEPT
```

- Если в качестве хранилища событий используется  
LogSpace:

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -
s <IP-адрес сервера Ankey SIEM NG Server> -p tcp --dport 8123 -m
conntrack --ctstate NEW -m comment --comment "From Ankey
SIEM NG Server to Ankey SIEM NG Events Storage" -j ACCEPT
```

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -
s <IP-адрес сервера Ankey SIEM NG Core> -p tcp --dport 8123 -m
conntrack --ctstate NEW -m comment --comment "From Ankey
SIEM NG Core to Ankey SIEM NG Events Storage" -j ACCEPT
```

**12. На серверах под управлением Linux заблокируйте все входящие  
соединения, кроме разрешенных:**

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -j DROP
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса>
-j REJECT
```

**13. Для сохранения созданных правил на серверах под управлением  
Debian установите пакет iptables-persistent: apt-get install iptables-  
persistent**

**Примечание.** Порядок сохранения правил на серверах под управлением Astra Linux описан в [справочном центре производителя операционной системы](#).

14. Сохраните правила межсетевого экрана: `netfilter-persistent save`
15. На серверах коллекторов под управлением Windows Server удалите все правила удаленного доступа по протоколу RDP:  
`netsh advfirewall firewall delete rule name=all protocol=tcp localport=3389`  
`netsh advfirewall firewall delete rule name=all protocol=udp localport=3389`
16. Разрешите удаленный доступ по протоколу RDP только с рабочих станций администраторов:  
`netsh advfirewall firewall add rule name="Allow RDP TCP in" dir=in action=allow protocol=tcp localport=3389 remoteip=<IP-адреса рабочих станций администраторов>`  
`netsh advfirewall firewall add rule name="Allow RDP UDP in" dir=in action=allow protocol=udp localport=3389 remoteip=<IP-адреса рабочих станций администраторов>`
17. Если для сбора событий по стандарту syslog и протоколу Netflow коллекторы на Windows Server не использует порты по умолчанию, на серверах коллекторов удалите правила для входящих соединений с этих портов:  
`for %P IN (514,1468) DO (netsh advfirewall firewall delete rule name=all protocol=tcp localport=%P)`  
`for %P IN (514,2055) DO (netsh advfirewall firewall delete rule name=all protocol=udp localport=%P)`
18. Разрешите входящие соединения для сбора событий по стандарту syslog и протоколу Netflow на серверах коллекторов на Linux для портов, указанных при создании задачи на сбор событий:  
`iptables -A INPUT -i <Название внешнего сетевого интерфейса> -p tcp -m tcp --dport 1468 -m conntrack --ctstate NEW -m comment --comment "Agent SysLog (TCP)" -j ACCEPT`  
`iptables -A INPUT -i <Название внешнего сетевого интерфейса> -p udp -m udp --dport 514 -m conntrack --ctstate NEW -m comment --comment "Agent SysLog (UDP)" -j ACCEPT`
19. Смените пароли служебных учетных записей в ПК Ankey SIEM NG (подробнее см. Руководство администратора Ankey SIEM NG 5.2.3).
20. На серверах под управлением Windows Server убедитесь, что пароли для входа в операционную систему соответствуют требованиям к сложности, установленным в организации.
21. Установите собственные доверенные сертификаты (см. подраздел 3.21) для Ankey SIEM NG Core, Knowledge Base, Ankey SIEM NG MC и RabbitMQ.
22. На серверах под управлением Linux для каждого администратора ПК Ankey SIEM NG создайте отдельную учетную запись:  
`adduser <Логин администратора>`

23. На рабочих станциях администраторов ПК Ankey SIEM NG настройте подключение по протоколу SSH с помощью ключей:

- сгенерируйте ключевую пару с помощью утилиты `ssh-keygen`, например:

```
ssh-keygen -o -a 100 -t ed25519 -f ~/.ssh/siem
```

где:

o – указание сохранить приватный ключ с использованием формата OpenSSH вместо PEM;

a – указание количества циклов KDF (Key Derivation Function, функция формирования ключа);

Высокие значения приведут к замедлению проверки парольной фразы, увеличивая её устойчивость к перебору при краже приватного ключа;

t – указание типа создаваемого ключа, например, с использованием алгоритма ed25519;

**Внимание!** Перед созданием ключевой пары убедитесь в том, что вы не используете название и путь, которые дублируют уже существующую пару ключей. Это позволит избежать случайной потери данных.

- введите и подтвердите пароль для ключевой пары;
- нажмите **Enter**, чтобы принять все внесенные изменения.

```
gis@core:~$ ssh-keygen -o -a 100 -t ed25519 -f ~/.ssh/siem
Generating public/private ed25519 key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/gis/.ssh/siem
Your public key has been saved in /home/gis/.ssh/siem.pub
The key fingerprint is:
SHA256:TNoLx3IPT7Cz... gis@core
The key's randomart image is:
+--[ED25519 256]--+
|
|
|
|
|
|
|
|
|
|
+---[SHA256]-----+
```

Рисунок 3.30 – Пример генерации пары ключей

- передайте открытый ключ с расширением `.pub` на удаленные серверы под управлением Linux, с которыми необходимо установить соединение:

```
ssh-copy-id -i <путь до открытого ключа>/<название открытого ключа>.pub <Логин администратора>@<адрес удаленного сервера>
```

Открытый ключ будет сохранен по пути

/home/<Логин администратора>/.ssh/authorized\_keys

- на каждом удаленном сервере в файле /etc/ssh/sshd\_config раскомментируйте и измените значения параметров (разрешите вход только с помощью SSH-ключей):

PubkeyAuthentication yes

RhostsRSAAuthentication no

HostbasedAuthentication no

PermitEmptyPasswords no

PasswordAuthentication no

- на каждом удаленном сервере в файле /etc/sudoers измените значение параметра:

<Логин администратора> ALL=(ALL) ALL

24. Для каждого пользователя ПК Ankey SIEM NG создайте отдельную учетную запись.

25. Смените пароль учетной записи Administrator34.

ПК Ankey SIEM NG настроен.

## 4 Обновление ПК Ankey SIEM NG

Вы можете обновлять компоненты ПК Ankey SIEM NG с помощью дистрибутивов.

Для обновления каждого компонента ПК Ankey SIEM NG требуется не менее 50 ГБ свободного места на жестком диске сервера. Если компоненты ПК Ankey SIEM NG установлены на одном сервере, требуется не менее 60 ГБ свободного места.

**Внимание!** Перед началом обновления создайте резервную копию данных компонентов.

Прежде чем приступить к обновлению ПК Ankey SIEM NG, рекомендуется остановить все задачи по сбору данных, а также убедиться, что на период обновления не запланирован запуск задач по расписанию. Это позволит избежать накопления очередей во время обновления, а также ошибок при выполнении задач после обновления.

Перед началом обновления необходимо убедиться в отсутствии ошибок в работе системы (индикатор состояния системы не красный).

Если вы используете удаленное подключение к серверам компонентов, рекомендуется не прерывать сессию удаленного подключения до завершения обновления. Для удаленного подключения к серверам на Linux рекомендуется использовать утилиту `screen`.

Иерархическую установку ПК Ankey SIEM NG необходимо обновлять в следующем порядке: сначала обновить компоненты, расположенные на главной площадке, и только затем – компоненты, расположенные на подчиненных площадках.

### 4.1 Обновление с помощью дистрибутивов

Компоненты Ankey SIEM NG Core, Ankey SIEM NG MC, Knowledge Base, Ankey SIEM NG Server и Ankey SIEM NG Events Storage установлены на Linux. Базовыми единицами установки и обновления являются роли (см. раздел 3.3).

Для обновления ПК Ankey SIEM NG необходимо обратиться в техническую поддержку ООО «Газинформсервис» и получить дистрибутивы с новыми версиями компонентов.

ПК Ankey SIEM NG необходимо обновлять в следующем порядке:

1. Обновление роли Deployer.
2. Обновление компонента Ankey SIEM NG MC.
3. Обновление компонента Knowledge Base.
4. Обновление компонента Ankey SIEM NG Core.
5. Обновление компонента Ankey SIEM NG Events Storage.
6. Обновление компонента Ankey SIEM NG Server (как стандартной, так и облегченной версии).
7. Обновление компонентов Ankey SIEM NG Collector.
8. Обновление компонента Ankey SIEM NG RC.

Для обновления компонентов на Linux используется сценарий `install.sh`, который необходимо запускать в интерфейсе терминала от имени суперпользователя (`root`).

В результате обновления роли (в том числе и неуспешного) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `/installReports` с отчетами об обновлении. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки.

#### 4.1.1 Обновление роли Deployer

**Внимание!** Для корректной работы Ankey SIEM NG необходимо, чтобы подсеть его Docker-контейнеров не совпадала с подсетями, используемыми в вашей организации. По умолчанию система виртуализации Docker использует подсеть 172.17.0.0/12. Вы можете изменить подсеть по инструкции из раздела «Подсеть Docker-контейнера Ankey SIEM NG совпадает с одной из подсетей предприятия» документа «Руководства администратора Ankey SIEM NG».

Для обновления роли вам потребуется архив `Deployer_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы обновить роль:

1. Распакуйте архив `Deployer_<Номер версии>.tar.gz`:  
`tar -xvf Deployer_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.  
Начнутся распаковка и подготовка пакетов. По завершении подготовки откроется окно с текстом лицензионного соглашения.
4. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.  
Откроется окно для проверки и изменения параметров установки.
5. Выберите вариант **Basic configuration**.  
Откроется страница со списком основных параметров.
6. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) или IPv4-адрес сервера, на который установлена роль Deployer.
7. Нажмите кнопку **OK**.  
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
8. Нажмите кнопку **OK**.
9. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль обновлена.

### 4.1.2 Обновление компонента Ankey SIEM NG MC на Linux

Компонент Ankey SIEM NG MC необходимо обновлять в следующем порядке: сначала обновить роль SqlStorage или JatobaStorage, затем – роль Management and Configuration.

#### 4.1.2.1 Обновление роли SqlStorage

Для обновления роли SqlStorage потребуется архив SqlStorage\_<Номер новой версии>.tar.gz, который содержится в дистрибутиве ПК Ankey SIEM NG.

Чтобы обновить роль SqlStorage:

1. На сервер с ролью Deployer скопируйте архив sqlstorage\_<Номер версии>.tar.gz.
2. Перейдите в каталог с архивом sqlstorage\_<Номер версии>.tar.gz и распакуйте его, выполнив команду `tar -xf sqlstorage_<Номер версии>.tar.gz`.
3. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
4. В открывшемся окне нажмите кнопку **Yes**. Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
5. Выберите вариант с идентификатором <идентификатор приложения, например, managementandconfiguration> или с тем названием, которое выбрал пользователь при создании приложения.
6. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. В открывшемся окне выберите вариант с названием экземпляра роли <название роли, например sqlstorage>. Откроется окно для проверки и изменения параметров установки.
8. Выберите вариант **Basic configuration**. Откроется страница со списком основных параметров.
9. Убедитесь, что в качестве значения параметра HostAddress указано полное доменное имя (FQDN) или IPv4-адрес сервера с компонентом Ankey SIEM NG Core.
10. Нажмите кнопку **OK**. Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
11. Нажмите кнопку **OK**.
12. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль SqlStorage обновлена.

#### 4.1.2.2 Обновление роли JatobaStorage

СУБД Jatoba функционирует в docker-контейнере. Перед началом обновления СУБД Jatoba может потребоваться новый лицензионный ключ. Вы можете получить актуальный ключ активации для новой лицензии СУБД Jatoba, отправив запрос на электронную почту [jatoba-support@gaz-is.ru](mailto:jatoba-support@gaz-is.ru).

**Примечание.** Если количество реактиваций ключа не исчерпано, то для реактивации возможно использовать этот же ключ.

Активация новой лицензии для СУБД Jatoba необходима в том случае, если при обновлении СУБД Jatoba обновляется версия docker-контейнера.

В процессе обновления роли JatobaStorage может потребоваться повторная активация лицензии для СУБД Jatoba, так как в процессе обновления СУБД Jatoba дополнительно обновляется и docker-контейнер, что приводит к нарушению условий лицензирования, из-за чего СУБД Jatoba внутри docker-контейнера перестает корректно функционировать.

Для обновления роли JatobaStorage потребуется архив `jatobastorage_<Номер новой версии>.tar.gz`, который содержится в дистрибутиве ПК Ankey SIEM NG.

Чтобы обновить роль JatobaStorage:

1. На сервер с ролью Deployer скопируйте архив `jatobastorage_<Номер версии>.tar.gz`.
2. Перейдите в каталог с архивом `jatobastorage_<Номер версии>.tar.gz` и распакуйте его, выполнив команду `tar -xf jatobastorage_<Номер версии>.tar.gz`.
3. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
4. В открывшемся окне нажмите кнопку **Yes**. Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
5. Выберите вариант с идентификатором `<идентификатор приложения, например, managementandconfiguration>` или с тем названием, которое выбрал пользователь при создании приложения.
6. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. В открывшемся окне выберите вариант с названием экземпляра роли `<название роли, например jatobastorage>`. Откроется окно для проверки и изменения параметров установки.
8. Выберите вариант **Advanced configuration**. Откроется страница со списком параметров установки.
9. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) или IPv4-адрес сервера с компонентом Ankey SIEM NG Core.
10. В поле **JatobaLicenseActivationType**, с помощью клавиши «Space/Пробел» выберите режим активации лицензии (**Online** или **Offline**).
11. В поле **LicenseKey** введите актуальный лицензионный ключ.

12. Нажмите кнопку **ОК**.  
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
13. Если не требуется корректировка дополнительных параметров, то с помощью стрелок на клавиатуре выполните переход на графическую кнопку **ОК** и нажмите клавишу «Ввод/Enter».
14. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль `JatobaStorage` обновлена.

Для повторной активации лицензии СУБД `Jatoba` следует выполнить инструкции, которые приведены в подразделе 3.7.3 или 3.7.4 в зависимости от типа активации, которая была выбрана при установке СУБД `Jatoba`.

**Внимание!** При активации лицензии в режиме офлайн файлы с расширением `.bak` в каталоге `/var/lib/deployedroles/<название приложения MC, например: mc-application-ankey>/<название роли СУБД Jatoba, например: jatobastorage>/config/license/` **следует игнорировать**.

#### 4.1.2.3 Обновление роли *Management and Configuration*

**Внимание!** Для получения обновлений экспертных данных Ankey SIEM NG<sup>35</sup> в изолированном сегменте сети без прямого подключения к интернету необходим локальный сервер обновлений, установленный и настроенный в соответствии с инструкциями в разделе «Настройка обновления экспертных данных» (см. раздел 3.23).

Для обновления роли вам потребуется архив `managementandconfiguration_<Номер версии>.tar.gz` из комплекта поставки и токен аутентификации, который хранится в файле `instance-access-token.key` и представляет собой набор символов, закодированных с использованием стандарта Base64. Этот набор символов необходимо будет указать в качестве значения конфигурационного параметра `PackagesSourceCredentialToken` на одном из шагов инструкции.

**Примечание.** Новые пользователи Ankey SIEM NG получают файл `instance-access-token.key` вместе с лицензией на продукт, а существующие пользователи, обновляющиеся с версии 4.1 – вместе с дистрибутивом или через службу технической поддержки.

❖ Чтобы обновить роль:

1. На сервере Ankey SIEM NG Core распакуйте архив `managementandconfiguration_<Номер версии>.tar.gz`:  
`tar -xvf managementandconfiguration_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.

<sup>35</sup> Центр обновлений экспертных данных Ankey SIEM NG доступен в исполнениях Ankey SIEM NG VM и Ankey SIEM NG с дополнительным компонентом VM

3. В открывшемся окне нажмите кнопку **Yes**.  
Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Management and Configuration.
5. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
6. В открывшемся окне выберите вариант с названием экземпляра роли Management and Configuration.  
Откроется окно для проверки и изменения параметров установки.
7. Выберите вариант **Basic configuration**.  
Откроется страница со списком основных параметров.
8. Убедитесь, что в качестве значения параметров HostAddress и PostgreHost указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Core.
9. В качестве значения параметра ExpertDataUpdateMethod выберите:

| для исполнения Ankey SIEM NG | для исполнения Ankey SIEM NG с дополнительным компонентом VM                                                                                                                                                                                                       |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Offline</b>               | <ul style="list-style-type: none"> <li>– если обновление экспертных данных будет осуществляться напрямую с сервера обновлений «Газинформсервис» или с помощью локального сервера обновлений – <b>Online.</b>;</li> <li>– если вручную – <b>Offline.</b></li> </ul> |

10. В качестве значения параметра PackagesSourceUri укажите:
  - если вы обновляете Ankey SIEM NG в сегменте сети с прямым подключением к интернету – адрес глобального сервера обновлений  
<https://update.ptsecurity.com/packman/v1/>;
  - если в изолированном сегменте сети без прямого подключения к интернету – адрес локального сервера обновлений в формате <http://<Адрес сервера>:<Порт>/packman/v1/>.

**Примечание.** Указанный в параметре порт локального сервера обновлений должен быть открыт для входящих соединений. Для подключения по протоколам HTTP и HTTPS по умолчанию используются порты 8553 и 8743 соответственно.

11. В качестве значения параметра PackagesSourceCredentialToken укажите содержимое файла instance-access-token.key.
12. Нажмите кнопку **OK**.  
Начнется установка пакетов. По завершении установки появится сообщение Deployment configuration successfully applied.
13. Нажмите кнопку **OK**.

Роль обновлена.

#### 4.1.3 Обновление компонента Knowledge Base на Linux

Для обновления компонента необходимо обновить роль Knowledge Base. Для обновления роли вам потребуется архив KB\_<Номер версии>.tar.gz из комплекта поставки.

❖ Чтобы обновить роль:

1. На сервере с установленной ролью Deployer распакуйте архив KB\_<Номер версии>.tar.gz:  
`tar -xf KB_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.  
Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Knowledge Base.
5. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
6. В открывшемся окне выберите вариант с названием экземпляра роли Knowledge Base.  
Откроется окно для проверки и изменения параметров установки.
7. Выберите вариант **Basic configuration**.  
Откроется страница со списком основных параметров.
8. Проверьте значения параметров:  
SiemAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Server>  
HostAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>  
PostgreHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>  
MCAddress: https://<FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:3334 CoreAddress: https://<FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:443
9. Нажмите кнопку **OK**.  
Запустится установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
10. Нажмите кнопку **OK**.
11. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль обновлена.

#### 4.1.4 Обновление компонента Ankey SIEM NG Core на Linux

Компонент необходимо обновлять в следующем порядке: сначала обновить роль RMQ Message Bus, затем – роль Core.

##### 4.1.4.1 Обновление роли RMQ Message Bus на сервере Ankey SIEM NG Core

Для обновления роли вам потребуется архив `rmqmessagebus_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы обновить роль:

1. На сервере с установленной ролью Deployer распакуйте архив `rmqmessagebus_<Номер версии>.tar.gz`:  
`tar -xf rmqmessagebus_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.  
Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
6. В открывшемся окне выберите вариант с названием экземпляра роли RMQ Message Bus, который установлен на сервер Ankey SIEM NG Core.  
Откроется окно для проверки и изменения параметров установки.
7. Выберите вариант **Basic configuration**.  
Откроется страница со списком основных параметров.
8. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Core.
9. Нажмите кнопку **OK**.  
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
10. Нажмите кнопку **OK**.
11. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль обновлена.

##### 4.1.4.2 Обновление роли Core

Для обновления роли вам потребуется архив `core_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы обновить роль:

1. На сервере Ankey SIEM NG Core распакуйте архив `Core_<Номер версии>.tar.gz`:  
`tar -xf Core_<Номер версии>.tar.gz`

2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.  
Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG
5. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их..
6. В открывшемся окне выберите вариант с названием экземпляра роли Core.  
Откроется окно для проверки и изменения параметров установки.
7. Выберите вариант **Basic configuration**.  
Откроется страница со списком основных параметров.
8. Проверьте значения параметров:  
HostAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>  
MCAddress: https://<FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:3334  
KBAddress: https://<FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:8091  
PostgreHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>  
RMQHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>  
SiemFrontendAddress: http://<FQDN или IPv4-адрес сервера Ankey SIEM NG Server>:8013>
9. Нажмите кнопку **OK**.  
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
10. Нажмите кнопку **OK**.
11. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль обновлена.

#### 4.1.5 Обновление версии 4.0 компонента Ankey SIEM NG Events Storage на Linux

**Внимание!** Перед обновлением компонента необходимо обновить роль Deployer.

Для обновления компонента необходимо обновить роль SIEM Storage.  
Порядок действий при обновлении зависит от типа установленного хранилища событий.

##### 4.1.5.1 Обновление роли Event Storage с хранилищем событий LogSpace

**Внимание!** Для установки или обновления роли Event Storage с хранилищем событий LogSpace на Debian необходима ОС на базе ядра Linux версии 5.10. Подробные инструкции по обновлению ядра можно найти на сайте производителя.

Для обновления роли вам потребуется архив `ankey_eventstorage_<Номер версии>.tar.gz` из комплекта поставки.

Чтобы обновить роль:

1. На сервере с установленной ролью **Deployer** распакуйте архив `ankey_eventstorage_<Номер версии>.tar.gz`:  
`tar -xf ankey_eventstorage_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.  
Начнется распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения **Ankey SIEM NG**.
5. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
6. В открывшемся окне выберите вариант с названием экземпляра роли **Event Storage**.  
Откроется окно для проверки и изменения параметров установки.
7. Выберите вариант **Basic configuration**.  
Откроется страница с перечнем параметров конфигурации.
8. В качестве значения параметра `Database` укажите название хранилища событий **LogSpace**.
9. В качестве значения параметра `PathData` укажите каталог хранилища событий **LogSpace**.
10. Нажмите кнопку **OK**.  
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
11. Нажмите кнопку **OK**.

Роль обновлена.

#### 4.1.5.2 Обновление роли **SIEM Storage** с хранилищем событий **Elasticsearch**

Для обновления роли вам потребуется архив `ankey_siemstorage_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы обновить роль:

1. На сервере с установленной ролью **Deployer** распакуйте архив `ankey_siemstorage_<Номер версии>.tar.gz`:  
`tar -xf ankey_siemstorage_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.  
Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения **Ankey SIEM NG**.
5. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.

6. В открывшемся окне выберите вариант с названием экземпляра роли SIEM Storage.  
Откроется окно для проверки и изменения параметров установки.
7. Выберите набор параметров:
  - если ПК Ankey SIEM NG развернут в конфигурации для низконагруженных или средненагруженных систем, выберите вариант **Basic configuration**;
  - если ПК Ankey SIEM NG развертывается в конфигурации для высоконагруженных систем, выберите вариант **Advanced configuration**.
 Откроется страница с перечнем параметров конфигурации.
8. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Events Storage.
9. Если требуется установить Ankey SIEM NG Events Storage на сервер с публичным IP-адресом, присвойте параметру `ElasticsearchGlobalAccess` значение `True`.  
Параметр **ElasticsearchGlobalAccess** доступен только в наборе параметров **Advanced configuration**.

**Внимание!** Использование сервера с публичным IP-адресом для Ankey SIEM NG Events Storage требует осторожности: если незащищенный сервер будет подключен к интернету, любой человек сможет скачать, изменить или удалить ваши данные.

10. Установите значение параметра **ClusterConfigurationProfile**:
  - если ПК Ankey SIEM NG развернут в конфигурации для низконагруженных систем, установите значение **AIO**;
  - если для средненагруженных систем – значение **SIEMandStorage**;
  - если для высоконагруженных систем с потоком событий до 20000 в секунду – **Standalone**;
  - если для высоконагруженных систем с потоком событий выше 20000 в секунду – **ManagedStorage**.
11. Если требуется, измените значения параметров в автоматически созданных каталогах:
  - `PathData`: <Каталог для хранения индексов>

**Примечание.** В высоконагруженных системах каталог используется для хранения индексов, находящихся в теплой стадии, а также для хранения счетчиков всех индексов.

- `PathDataHot`: <Каталог для хранения индексов, находящихся в горячей стадии>

**Примечание.** Каталог используется только для высоконагруженных систем.

- PathRepo: <Каталог для хранения резервных копий индексов>
  - PathLog: <Каталог для хранения файлов журналов>
12. Если ПК Ankey SIEM NG развернут в конфигурации для высоконагруженных систем и сервер Ankey SIEM NG Events Storage имеет емкость ОЗУ 256 ГБ или более, установите флажок **HighLoad**.

**Примечание.** В случае установки флажка **HighLoad** кластер Elasticsearch будет содержать четыре узла данных.

13. Нажмите кнопку **OK**.  
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
14. Нажмите кнопку **OK**.
15. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль обновлена.

#### 4.1.6 Обновление версии 4.0 компонента Ankey SIEM NG Server на Linux

**Внимание!** Перед обновлением компонента необходимо обновить роль Deployer.

Если ПК Ankey SIEM NG развернут в конфигурации для средненагруженных или высоконагруженных систем, Ankey SIEM NG Server необходимо обновлять в следующем порядке: сначала обновить роль RMQ Message Bus, затем – роль SIEM Server. Если ПК Ankey SIEM NG развернут в конфигурации для низконагруженных систем, необходимо обновить только роль SIEM Server.

##### 4.1.6.1 Обновление роли RMQ Message Bus на сервере Ankey SIEM NG Server

Для обновления роли вам потребуется архив `rmqmessagebus_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы обновить роль:

1. На сервере с установленной ролью Deployer распакуйте архив `rmqmessagebus_<Номер версии>.tar.gz`:  
`tar -xf rmqmessagebus_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.  
Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.

6. В открывшемся окне выберите вариант с названием экземпляра роли RMQ Message Bus, который установлен на сервер Ankey SIEM NG Server.  
Откроется окно для проверки и изменения параметров установки.
7. Выберите вариант **Basic configuration**.  
Откроется страница со списком основных параметров.
8. Убедитесь, что в качестве значения параметра HostAddress указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Server.
9. Нажмите кнопку **OK**.  
Начнется установка пакетов. По завершении установки появится сообщение Deployment configuration successfully applied.
10. Нажмите кнопку **OK**.
11. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль обновлена.

#### 4.1.6.2 Обновление роли SIEM Server

Для обновления роли вам потребуется архив siemserver-linux\_<Номер версии>.tar.gz из комплекта поставки.

Перед обновлением роли SIEM Server необходимо изменить конфигурацию роли, выбрав для параметра TableListsRestorePolicy вариант robust.

❖ Чтобы обновить роль:

1. На сервере с установленной ролью Deployer распакуйте архив siemserver-linux\_<Номер версии>.tar.gz:  
tar -xvf siemserver-linux\_<Номер версии>.tar.gz
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли ./install.sh.
3. В открывшемся окне нажмите кнопку **Yes**.  
Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
6. В открывшемся окне выберите вариант с названием экземпляра роли SIEM Server.  
Откроется окно для проверки и изменения параметров установки.
7. Выберите вариант **Advanced configuration**.  
Откроется страница со списком параметров (см. приложение Б).
8. Укажите значения параметров:  
CoreAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>  
HostAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Server>  
RMQHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>
9. Проверьте значение параметра **StorageBackendType**:  
– если для хранения событий используется Elasticsearch, убедитесь, что выбран вариант **elasticsearch**;

- если используется LogSpace – выбран вариант **logspace**.
- 10. Если ПК Ankey SIEM NG развернут в конфигурации для высоконагруженных систем, проверьте значение параметра, указывающего расположение сервера Ankey SIEM NG Events Storage в сети:
  - если для хранения событий используется Elasticsearch, проверьте значение параметра ElasticsearchHost:  
ElasticsearchHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Events Storage>
  - если используется LogSpace – проверьте значение параметра LogSpaceHost:  
LogSpaceHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Events Storage>
- 11. Если ПК Ankey SIEM NG развернут в конфигурации для высоконагруженных систем с потоком событий выше 20000 в секунду, убедитесь, что установлен флажок **ManagedStorage**.
- 12. Если предполагаемый поток событий от источников будет превышать 20 000 событий в секунду и сервер Ankey SIEM NG Events Storage имеет емкость ОЗУ 256 ГБ или более, убедитесь, что установлен флажок **HighLoad**.

**Примечание.** В случае установки флажка **HighLoad** для службы SIEM server storage будет выделено шесть потоков операционной системы (вместо четырех, когда флажок снят).

- 13. Нажмите кнопку **ОК**.  
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
- 14. Нажмите кнопку **ОК**.
- 15. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль обновлена.

#### 4.1.7 Обновление облегченной версии компонента Ankey SIEM NG Server на Linux

Облегченную версию Ankey SIEM NG Server необходимо обновлять в следующем порядке: сначала обновить роль RMQ Message Bus, затем – роль SIEM Server.

##### 4.1.7.1 Обновление роли RMQ Message Bus на сервере облегченной версии Ankey SIEM NG Server

Для обновления роли вам потребуется архив `rmqmessagebus_<Номер версии>.tar.gz` из комплекта поставки.

Чтобы обновить роль:

1. На сервере с установленной ролью Deployer распакуйте архив `rmqmessagebus_<Номер версии>.tar.gz`:  
`tar -xf rmqmessagebus_<Номер версии>.tar.gz`

2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
  3. В открывшемся окне нажмите кнопку **Yes**.  
Начнутся распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
  4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
  5. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
  6. В открывшемся окне выберите вариант с названием экземпляра роли `RMQ Message Bus`, который установлен на сервер облегченной версии Ankey SIEM NG Server.  
Откроется окно для проверки и изменения параметров установки.
  7. Выберите вариант **Basic configuration**.  
Откроется страница со списком основных параметров.
  8. Укажите в качестве значения параметра `HostAddress` `FQDN` или IPv4-адрес сервера облегченной версии Ankey SIEM NG Server.
  9. Нажмите кнопку **OK**.
  10. Начнется установка пакетов.  
По завершении установки появится сообщение `Deployment configuration successfully applied`.
  11. Нажмите кнопку **OK**.
- Роль обновлена.

#### 4.1.7.2 Обновление роли SIEM Server для облегченной версии компонента

Для обновления роли вам потребуется архив `siemserver-linux_<Номер версии>.tar.gz` из комплекта поставки.

Перед обновлением роли SIEM Server необходимо изменить конфигурацию роли, выбрав для параметра `TableListsRestorePolicy` вариант `robust`.

Чтобы обновить роль:

1. На сервере с установленной ролью `Deployer` распакуйте архив `siemserver-linux_<Номер версии>.tar.gz`:  
`tar -xf siemserver-linux_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.  
Начнутся распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
6. В открывшемся окне выберите название экземпляра роли SIEM Server облегченной версии компонента и нажмите кнопку **OK**.  
Откроется окно для проверки и изменения параметров установки.
7. Выберите набор параметров **Advanced configuration**.

Откроется страница с перечнем всех доступных параметров конфигурации.

8. Укажите значения параметров:  
HostAddress: <FQDN или IPv4-адрес сервера облегченной версии компонента Ankey SIEM NG Server>  
TargetSiemRabbitHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Server, который получает данные о событиях от облегченной версии компонента>
9. Установите флажок **SiemOnAgent**.
10. Если ПК Ankey SIEM NG развернут в конфигурации для высоконагруженных систем с потоком событий выше 20000 в секунду, установите флажок **ManagedStorage**.
11. Нажмите кнопку **ОК**.  
Начнется установка пакетов. По завершении установки появится сообщение *Deployment configuration successfully applied*.
12. Нажмите кнопку **ОК**.
13. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль обновлена.

#### 4.1.8 Обновление облегченной версии компонента Ankey SIEM NG Server на Microsoft Windows

**Внимание!** В результате обновления компонентов установленные ранее пользовательские сертификаты безопасности будут заменены сертификатами из комплекта поставки. Если для работы компонентов использовались сертификаты безопасности, отличные от стандартных, необходимо снова настроить их после обновления.

Для обновления вам потребуется архив `siemserver-windows_<Номер версии>.tar.gz` из комплекта поставки.

Чтобы обновить облегченную версию компонента Ankey SIEM NG Server:

1. Распакуйте архив `siemserver-windows_<Номер версии>.tar.gz`
2. Скопируйте файл `AnkeySiemSetup_<Номер версии>.exe` на сервер облегченной версии Ankey SIEM NG Server.
3. Запустите файл `AnkeySiemSetup_<Номер версии>.exe`.
4. Откроется окно мастера обновления.
5. Ознакомьтесь по ссылке с текстом лицензионного соглашения.
6. Установите флажок **Я принимаю условия лицензионного соглашения** и нажмите кнопку **Обновить**.
7. По завершении обновления нажмите кнопку **Заккрыть**.
8. Если стандартная версия Ankey SIEM NG Server установлена на Linux, скопируйте файл `/opt/deployer/pki/CAbundle.crt` с сервера, на котором установлена роль `Deployer`, на сервер облегченной версии Ankey SIEM NG Server.
9. Если стандартная версия Ankey SIEM NG Server установлена на Linux, скопируйте файлы  
`/var/lib/deployed-roles/<Идентификатор приложения Ankey SIEM NG Server>/<Название экземпляра роли SIEM`

Server>/certs/RMQ\_SIEM\_Client.crt и /var/lib/deployed-roles/<Идентификатор приложения Ankey SIEM NG Server>/<Название экземпляра роли SIEM Server>/certs/RMQ\_SIEM\_Client.key с сервера стандартной версии Ankey SIEM NG Server на сервер облегченной версии Ankey SIEM NG Server.

10. На сервере облегченной версии Ankey SIEM NG Server в интерфейсе командной строки Windows от имени администратора выполните команды:

```
coreagentcfg set -p AgentRMQVirtualHost siem RMQHost localhost
rabbitmqcfg set -p CACertFile <Путь к файлу CABundle.crt> -v
siemcfg set -p TargetSiemRabbitHost <IP-адрес или FQDN стандартной
версии Ankey SIEM NG Server> RMQHost <IP-адрес или FQDN
стандартной версии Ankey SIEM NG Server> RMQ_SSL_CA_CERTIFICATE
<Путь к файлу CABundle.crt> RMQ_SSL_CERTIFICATE <Путь к файлу
RMQ_SIEM_Client.crt> RMQ_SSL_KEY <Путь к файлу
RMQ_SIEM_Client.key>
```

11. Если стандартная версия Ankey SIEM NG Server установлена на Microsoft Windows, в интерфейсе командной строки Windows от имени администратора выполните команды:

```
coreagentcfg set -p AgentRMQVirtualHost siem RMQHost localhost
siemcfg set -p TargetSiemRabbitHost <IP-адрес или FQDN стандартного
Ankey SIEM NG Server, который будет получать данные о событиях от
облегченной версии компонента> RMQHost <IP-адрес или FQDN
стандартного Ankey SIEM NG Server, который будет получать данные о
событиях от облегченной версии компонента>
```

Облегченная версия компонента Ankey SIEM NG Server обновлена.

#### 4.1.9 Обновление правил нормализации и агрегации для облегченной версии Ankey SIEM NG Server

❖ Чтобы обновить правила нормализации и агрегации для облегченной версии Ankey SIEM NG Server:

1. В главном меню нажмите  и в раскрывшемся меню выберите пункт **Knowledge Base**.  
Откроется страница **Статистика**.

**Примечание.** Если вы используете браузер Mozilla Firefox и на странице **Статистика** отображается сообщение "Отключен", необходимо проверить, что адреса <https://<FQDN или IPv4-адрес компонента Ankey SIEM NG Core>:8091> добавлены в исключения безопасности браузера.

2. В главном меню в разделе <Название БД> выберите пункт **Базы данных**.  
Откроется страница **Базы данных / <Название БД>**.
3. В панели **Базы данных** выберите родительскую базу данных, которая содержит устанавливаемые правила.
4. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.

5. В панели **Папки** выберите **Все объекты**.
6. В панели **Наборы для установки** выберите **Все объекты**.
7. В панели со списком объектов нажмите .  
Появится строка с названиями фильтров.
8. По ссылке **Объекты: все** установите флажки **Агрегация** и **Нормализация**.
9. Повторно нажмите на ссылку.
10. В списке правил выберите те правила, которые требуется обновить для облегченной версии Ankey SIEM NG Server.

**Примечание.** Для выбора нескольких объектов подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных объектов – клавишу Ctrl, для выбора всех объектов в списке – комбинацию клавиш Ctrl+A.

11. Нажмите .  
Откроется окно **Экспорт объектов**.
12. Выберите вариант **Для установки в SIEM Lite**.
13. Нажмите кнопку **Экспортировать**.  
Браузер сохранит архив knowledgebase\_<Дата экспорта>.zip в папку загрузки.
14. Переместите файл архива на сервер облегченной версии Ankey SIEM NG Server в любую папку.
15. Если облегченная версия Ankey SIEM NG Server установлена на Linux, запустите установку правил нормализации и агрегации:  
"/opt/siem/bin/siemlight-kb" -u <Путь к файлу архива>

Правила нормализации и агрегации для облегченной версии Ankey SIEM NG Server обновлены.

#### 4.1.10 Обновление компонента Ankey SIEM NG Collector на Linux

Для обновления компонента необходимо обновить роль Collector. Для обновления роли вам потребуется архив agent-linux\_<Номер версии>.tar.gz из комплекта поставки.

❖ Чтобы обновить роль:

1. На сервере с установленной ролью Deployer распакуйте архив agent-linux\_<Номер версии>.tar.gz:  
tar -xf agent-linux\_<Номер версии>.tar.gz
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли ./install.sh.
3. В открывшемся окне нажмите кнопку **Yes**.  
Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.

6. В открывшемся окне выберите вариант с названием экземпляра роли Collector.  
Откроется окно для проверки и изменения параметров установки.
7. Выберите вариант **Advanced configuration**.  
Откроется страница со списком параметров.
8. Убедитесь, что в качестве значения параметра `AgentRMQHost` указано полное доменное имя (FQDN) или IPv4-адрес стандартной или облегченной версии Ankey SIEM NG Server – в зависимости от того, для какой версии компонента предназначен Ankey SIEM NG Collector.
9. В качестве значения параметра `AgentRMQVirtualHost` выберите `Siem`.
10. Нажмите кнопку **OK**.  
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
11. Нажмите кнопку **OK**.
12. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль обновлена.

#### 4.1.11 Обновление компонента Ankey SIEM NG Collector на Microsoft Windows

**Внимание!** В результате обновления компонентов установленные ранее пользовательские сертификаты безопасности будут заменены сертификатами из комплекта поставки. Если для работы компонентов использовались сертификаты безопасности, отличные от стандартных, необходимо снова настроить их после обновления.

Для обновления вам потребуется архив `agent-windows_<Номер версии>.tar.gz` из комплекта поставки.

Чтобы обновить компонент Ankey SIEM NG Collector:

1. Запустите файл `AnkeyAgentSetup_<Номер версии>.exe`.  
Откроется окно мастера обновления.
2. Ознакомьтесь по ссылке с текстом лицензионного соглашения.
3. Установите флажок **Я принимаю условия лицензионного соглашения** и нажмите кнопку **Обновить**.
4. По завершении обновления нажмите кнопку **Заккрыть**.
5. В командной строке Microsoft Windows выполните команду от имени администратора:  
`coreagentcfg set -p RMQHost <IP-адрес или FQDN сервера стандартной или облегченной версии Ankey SIEM NG Server>`

Компонент Ankey SIEM NG Collector обновлен.

#### 4.1.12 Обновление версии 4.0 компонента Ankey SIEM NG RC

Компонент необходимо обновлять в следующем порядке: сначала обновить роль RMQ Message Bus, затем – роль Retro Correlator.

##### 4.1.12.1 Обновление роли RMQ Message Bus на сервере Ankey SIEM NG RC

Для обновления роли вам потребуется архив `rmqmessagebus_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы обновить роль:

1. На сервере с установленной ролью Deployer распакуйте архив `rmqmessagebus_<Номер версии>.tar.gz`:  
`tar -xf rmqmessagebus_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.  
Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
6. В открывшемся окне выберите вариант с названием экземпляра роли RMQ Message Bus, который установлен на сервер Ankey SIEM NG RC.  
Откроется окно для проверки и изменения параметров установки.
7. Выберите вариант **Basic configuration**.  
Откроется страница со списком основных параметров.
8. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG RC.
9. Нажмите кнопку **OK**.  
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
10. Нажмите кнопку **OK**.

Роль обновлена.

##### 4.1.12.2 Обновление роли Retro Correlator

Для обновления роли вам потребуется архив `retrocorrelator_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы обновить роль:

1. На сервере с установленной ролью Deployer распакуйте архив `retrocorrelator_<Номер версии>.tar.gz`:  
`tar -xf retrocorrelator_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.

Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.

4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.
6. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG RC.
8. В открывшемся окне введите название экземпляра роли Retro Correlator и нажмите кнопку **OK**.  
Откроется окно для проверки и изменения параметров установки.
9. Выберите вариант **Basic configuration**.  
Откроется страница со списком основных параметров.
10. Проверьте значения параметров:  
HostAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG RC>  
InternalRMQHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG RC>  
CoreAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>  
KBAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:8091  
SiemServerAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Server>
11. Нажмите кнопку **OK**.  
Начнется установка пакетов. По завершении установки появится сообщение **Deployment configuration successfully applied**.
12. Нажмите кнопку **OK**.

Роль обновлена.

## 5 Удаление компонентов из ОС Windows

❖ Для удаления компонентов Ankey SIEM NG Collector и облегченной версии Ankey SIEM NG Server в среде Windows вы можете использовать стандартные средства ОС Windows. При удалении компонентов ПК Ankey SIEM NG вы можете также удалить пользовательские данные.

### **Удаление компонента ПК Ankey SIEM NG стандартными средствами ОС Windows**

❖ Чтобы удалить компонент Ankey SIEM NG Collector или облегченную версию Ankey SIEM NG Server:

1. В контекстном меню кнопки **Пуск** выберите пункт **Программы и компоненты**.
2. В списке установленных программ выберите компонент ПК Ankey SIEM NG и нажмите кнопку **Удалить/Изменить**.  
Откроется окно мастера удаления компонента ПК Ankey SIEM NG.
3. Нажмите кнопку **Удалить**.
4. Если требуется удалить пользовательские данные, установите флажок **Удалить данные приложений**.
5. Нажмите кнопку **Удалить**.  
Запустится процесс удаления компонента ПК Ankey SIEM NG.
6. По завершении удаления нажмите кнопку **Заккрыть**.

Компонент ПК Ankey SIEM NG удален.

## 6 Диагностика и решение проблем

Инструкции по диагностике и решению проблем, возникающих при работе с ПК Ankey SIEM NG, представлены в документе «Руководство администратора Ankey SIEM NG 5.2.3».

Если выполнение указанных в документе шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис».

**Примечание.** Порядок обращения в службу технической поддержки, а также особенности и ограничения услуг технической поддержки представлены в документе «Руководство администратора Ankey SIEM NG 5.2.3».

## Перечень сокращений

|       |   |                                                                                                                                                                |
|-------|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AIO   | – | All in One – конфигурация ПК Ankey SIEM NG для низконагруженных систем. Все компоненты устанавливаются на одном сервере                                        |
| API   | – | Application Programming Interface – протокол для взаимодействия компьютерных программ, который позволяет использовать функции одного приложения внутри другого |
| AVX   | – | Advanced Vector Extensions (AVX) – расширение системы команд x86 для микропроцессоров Intel и AMD                                                              |
| BIOS  | – | Basic Input/Output System – набор микропрограмм, реализующих низкоуровневые API для работы с аппаратным обеспечением компьютера                                |
| CIDR  | – | Classless Inter-Domain Routing – бесклассовая адресация                                                                                                        |
| CSV   | – | Comma-Separated Values – текстовый формат, предназначенный для представления табличных данных                                                                  |
| DMZ   | – | Demilitarized Zone – Демилитаризованная Зона (ДМЗ) – часть локальной сети, доступная из интернета и изолированная от других ресурсов.                          |
| DNS   | – | Domain Name System – компьютерная распределённая система для получения информации о доменах                                                                    |
| EPS   | – | Events Per Second – количество событий в секунду                                                                                                               |
| ES    | – | Компонент Ankey SIEM Next Generation Events Storage                                                                                                            |
| FQDN  | – | Fully Qualified Domain Name – имя домена, не имеющее неоднозначностей в определении                                                                            |
| HDD   | – | Hard disk drive – запоминающее устройство                                                                                                                      |
| HTML  | – | HyperText Markup Language – стандартизированный язык гипертекстовой разметки                                                                                   |
| HTTP  | – | HyperText Transfer Protocol – протокол передачи гипертекста                                                                                                    |
| HTTPS | – | HyperText Transfer Protocol Secure – расширение протокола HTTP в целях повышения уровня безопасности                                                           |

|      |   |                                                                                                                                                                                                                                                                                                  |
|------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ILM  | – | Information Lifecycle Management – перемещение информации различного рода и ценности в системе хранения данных (СХД) на основании модифицирующихся требований бизнеса к критериям защищенности и доступности информации с учетом ее ценности, актуальности и оптимизации расходов на ее хранение |
| IOPS | – | Input/output operations per second – количество операций ввода-вывода в секунду                                                                                                                                                                                                                  |
| IP   | – | Internet Protocol – маршрутизируемый протокол сетевого уровня стека TCP/IP                                                                                                                                                                                                                       |
| KB   | – | Knowledge Base – это единая база знаний ПК Ankey SIEM NG                                                                                                                                                                                                                                         |
| LDAP | – | Lightweight Directory Access Protocol – протокол прикладного уровня для доступа к службе каталогов X.500, разработанный IETF как облегченный вариант разработанного ИТУ-Т протокола DAP                                                                                                          |
| LUS  | – | Local Update Server, Локальный сервер обновлений Ankey SIEM NG                                                                                                                                                                                                                                   |
| MC   | – | Компонент Ankey SIEM NG Management and Configuration                                                                                                                                                                                                                                             |
| NFS  | – | Network File System – протокол сетевого доступа к файловым системам                                                                                                                                                                                                                              |
| ODBC | – | Open Database Connectivity – программный интерфейс (API) доступа к базам данных                                                                                                                                                                                                                  |
| PDQL | – | Язык, разработанный для написания запросов в процессе обработки событий, инцидентов, динамических групп активов и табличных списков в ПК Ankey SIEM NG                                                                                                                                           |
| PEM  | – | Privacy Enhanced Mail Certificate – сертификат, зашифрованный в Base64, широко применяемый как формат категории интернет-файлов                                                                                                                                                                  |
| RC   | – | Компонент Ankey SIEM NG Retro Correlator                                                                                                                                                                                                                                                         |
| RDP  | – | Remote Desktop Protocol – протокол удаленного рабочего стола                                                                                                                                                                                                                                     |
| RSA  | – | Rivest, Shamir и Adleman – криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел                                                                                                                                      |

|       |   |                                                                                                                                                                                                                                              |
|-------|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RTO   | – | Recovery Time Objective – допустимое время восстановления данных                                                                                                                                                                             |
| SAN   | – | Subject Alternative Name – расширение X.509, позволяющее связать различные значения с сертификатом безопасности с помощью поля subjectAltName                                                                                                |
| SAS   | – | Serial Attached SCSI – последовательный компьютерный интерфейс, разработанный для подключения различных устройств хранения данных                                                                                                            |
| SATA  | – | Serial ATA – последовательный интерфейс обмена данными с накопителями информации                                                                                                                                                             |
| SCADA | – | Supervisory Control And Data Acquisition – программный пакет, предназначенный для разработки или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте мониторинга или управления |
| SHA   | – | Secure Hash Algorithm – семейство криптографических хеш-функций                                                                                                                                                                              |
| SIEM  | – | Security information and event management – класс программных продуктов, предназначенных для сбора и анализа информации о событиях безопасности                                                                                              |
| SMTP  | – | Simple Mail Transfer Protocol – сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP                                                                                                                              |
| SOC   | – | Security operations center – центр управления безопасностью отвечает за защиту организации от киберугроз                                                                                                                                     |
| SSD   | – | Solid-State Drive – компьютерное энергонезависимое немеханическое запоминающее устройство на основе микросхем памяти                                                                                                                         |
| SSH   | – | Secure Shell – сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений                                                                                       |
| SSL   | – | Secure Sockets Layer – криптографический протокол, который подразумевает более безопасную связь                                                                                                                                              |
| TCP   | – | Transmission Control Protocol – протокол передачи данных интернета                                                                                                                                                                           |

|        |   |                                                                                    |
|--------|---|------------------------------------------------------------------------------------|
| TLS    | – | Transport Layer Security – криптографический протокол, основанный на протоколе SSL |
| TTL    | – | Time To Live, время актуальности данных                                            |
| TXT    | – | Компьютерный файл, содержащий текстовые данные                                     |
| UDP    | – | User Datagram Protocol – протокол транспортного уровня                             |
| VM     | – | Vulnerability Management, дополнительный компонент Ankey SIEM NG                   |
| АСУ ТП | – | Автоматизированная система управления технологическим процессом                    |
| БД     | – | База данных                                                                        |
| ИБ     | – | Информационная безопасность                                                        |
| ИТ     | – | Информационные технологии                                                          |
| ОЗУ    | – | Оперативное запоминающее устройство                                                |
| ОС     | – | Операционная система                                                               |
| ПК     | – | Программный комплекс                                                               |
| СУБД   | – | Система управления базами данных                                                   |
| ЦС     | – | Центр сертификации                                                                 |

## Приложение А

### Порядок установки ПК Ankey SIEM NG

Пример распределения ролей и алгоритма инсталляции по серверам ПК Ankey SIEM NG в низконагруженной конфигурации представлен на рисунке А.1.

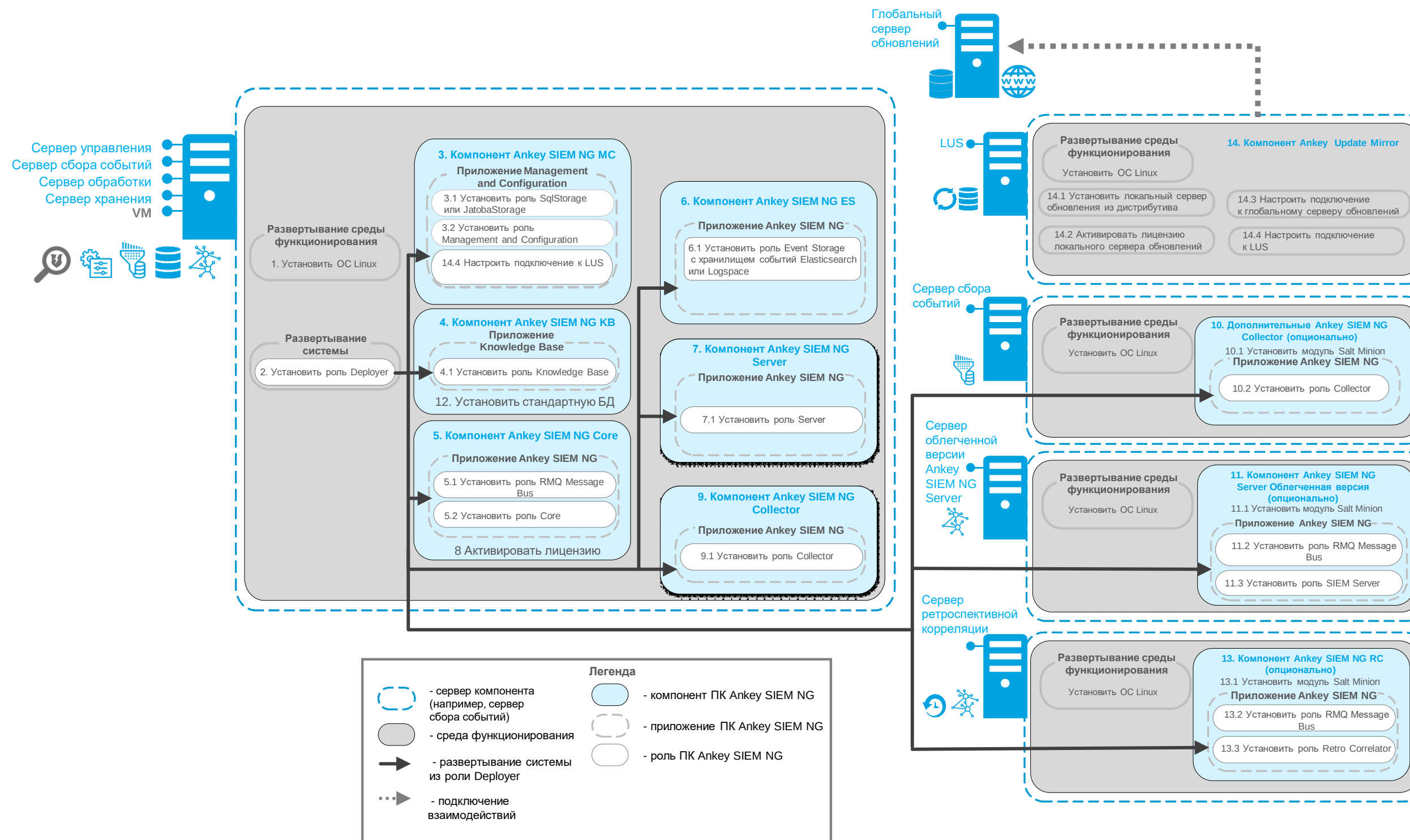


Рисунок А.1 – Алгоритм инсталляции ПК Ankey SIEM NG в низконагруженной конфигурации

Пример распределения ролей и алгоритма инсталляции по серверам ПК Ankey SIEM NG в средненагруженной конфигурации представлен на рисунке А.2.

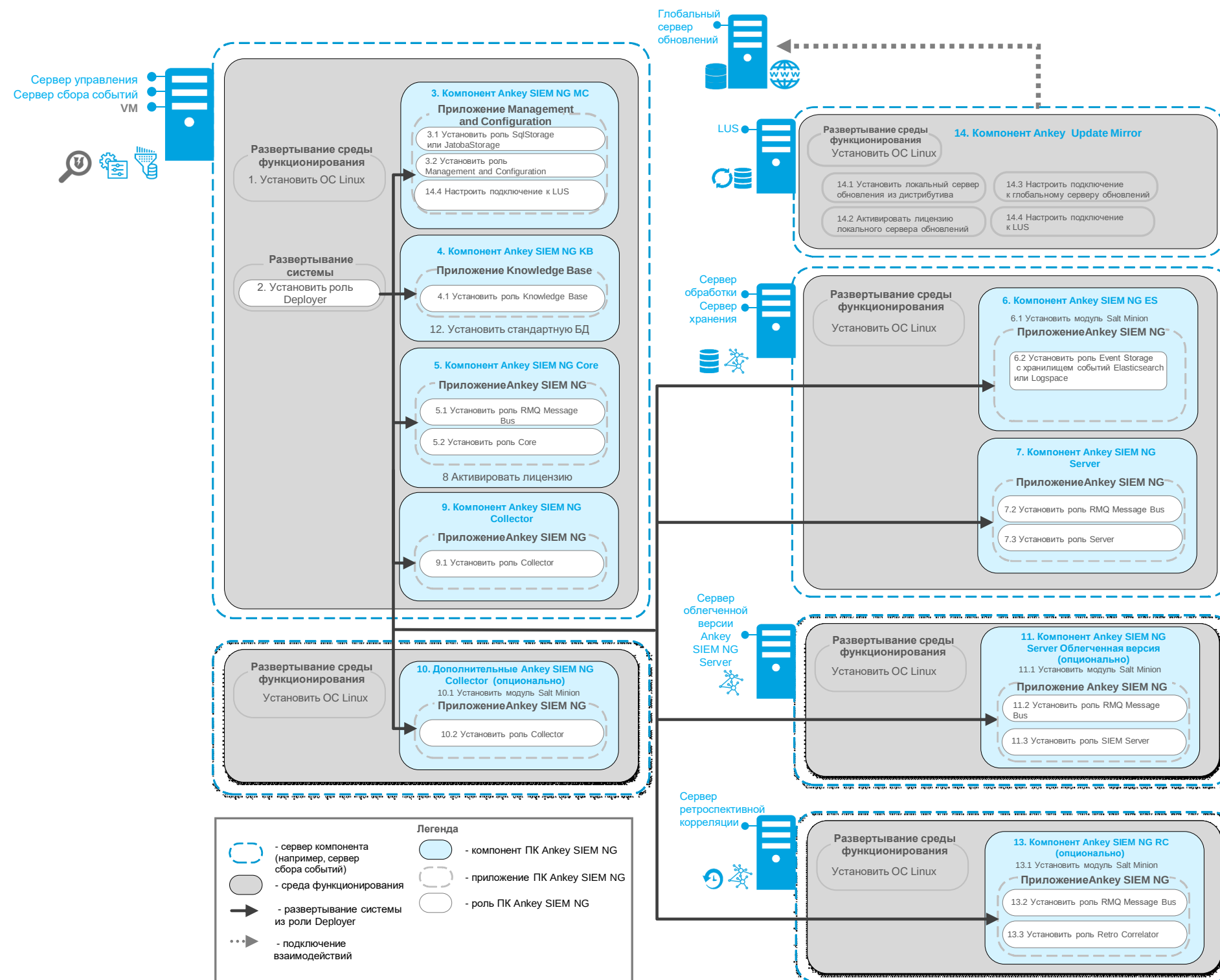


Рисунок А.2 – Алгоритм инсталляции ПК Ankey SIEM NG в средненагруженной конфигурации

Пример распределения ролей и алгоритма инсталляции по серверам ПК Ankey SIEM NG в высоконагруженной конфигурации представлен на рисунке А.3.

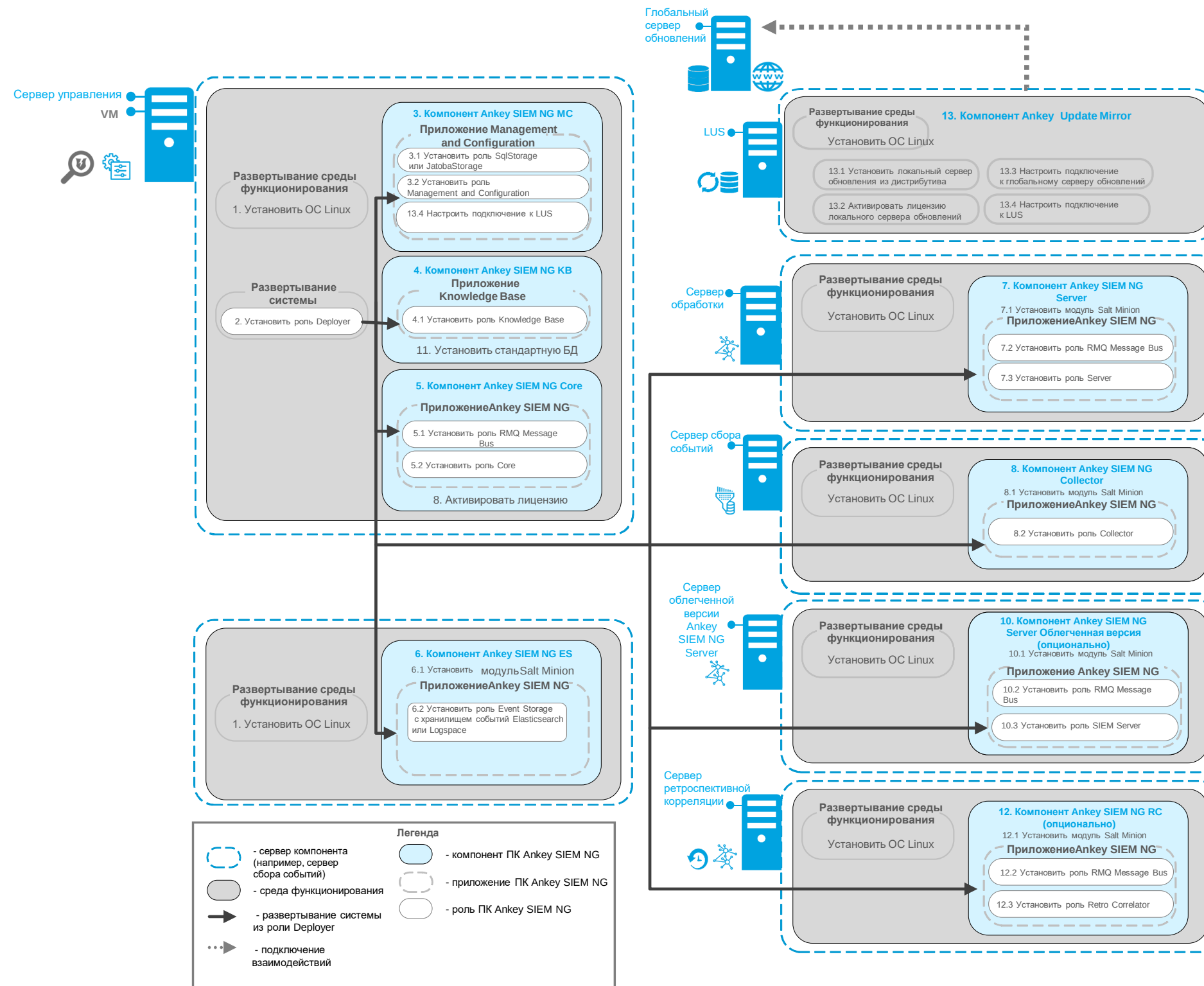


Рисунок А.3 – Алгоритм инсталляции ПК Ankey SIEM NG в высоконагруженной конфигурации

## Приложение Б

### Параметры конфигурации компонентов ПК Ankey SIEM NG на Linux

В этом приложении приведены описания параметров и их значения по умолчанию.

Таблица Б.1 – Параметры конфигурации роли Deployer

| Параметр                | Описание                                                                                                                                                              | Значение по умолчанию |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| CustomDockerAddressPool | Подсеть Docker, которую необходимо использовать для Docker-контейнеров вместо подсети по умолчанию                                                                    | –                     |
| CustomDockerNetworkSize | Размер подсетей, которые будут выделяться из диапазона, указанного в параметре CustomDockerAddressPool.<br>Рекомендуется использовать значение, не превышающее 25 бит | –                     |
| HostAddress             | IP-адрес или FQDN сервера с установленной ролью Deployer                                                                                                              | –                     |
| RegistryBindHost        | IP-адрес или FQDN сервера с локальным реестром Docker-образов                                                                                                         | –                     |
| RegistryPort            | Номер порта для доступа к локальному реестру Docker-образов                                                                                                           | 5000                  |

Таблица Б.2 – Параметры конфигурации роли SqlStorage и JatobaStorage

| Параметр                                      | Описание                                                                                       | Значение по умолчанию                       |
|-----------------------------------------------|------------------------------------------------------------------------------------------------|---------------------------------------------|
| <b>Параметры конфигурации роли SqlStorage</b> |                                                                                                |                                             |
| CACertificateFileName                         | Имя файла корневого сертификата                                                                | rootCA.crt                                  |
| CollectorAgentHttpPort                        | Порт для доступа к коллектору OpenTelemetry в роли SqlStorage/JatobaStorage по протоколу HTTP  | 4319                                        |
| CollectorAgentSyslogUdpPort                   | Порт для прослушивания журналов syslog по протоколу UDP                                        | 54528                                       |
| DockerRegistry                                | Порт для доступа к реестру Docker-образов                                                      | Адрес сервера компонента Ankey SIEM NG Core |
| EnableFilesLogCollection                      | Запись журналов в файл вместо их централизованного сбора включена (True) или выключена (False) | False                                       |
| HostAddress                                   | IP-адрес или FQDN сервера с установленной ролью SqlStorage/JatobaStorage                       | –                                           |
| Network                                       | Сетевое имя реестра Docker-образов                                                             | storage-network.sqlstorage                  |

| Параметр             | Описание                                                                                                                                                                                                                                                                                                                                                                      | Значение по умолчанию |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| NetworkDriver        | Драйвер Docker-образов                                                                                                                                                                                                                                                                                                                                                        | bridge                |
| PgAdminPort          | Порт для доступа к PgAdmin                                                                                                                                                                                                                                                                                                                                                    | 9001                  |
| PgAnalyzeScaleFactor | Доля от числа кортежей в таблице, которая прибавляется к значению параметра PgAnalyzeThreshold при расчете порога срабатывания команды ANALYZE. Например, если значение PgAnalyzeThreshold равно 200 000, а значение параметра PgAnalyzeScaleFactor равно 0,1, то для таблицы в 1 000 000 кортежей порог срабатывания команды будет $200\,000 + 100\,000 = 300\,000$ кортежей | 0.0                   |
| PgAnalyzeThreshold   | Минимальное число добавленных, измененных или удаленных кортежей, при котором будет выполняться команда ANALYZE для отдельно взятой таблицы                                                                                                                                                                                                                                   | 200000                |
| PgEffectiveCacheSize | Эффективный размер дискового кэша, доступный для одного запроса                                                                                                                                                                                                                                                                                                               | 6GB                   |
| PgEmail              | Электронный адрес служебной учетной записи для доступа к СУБД PostgreSQL                                                                                                                                                                                                                                                                                                      | email@email.com       |
| PgHardDiskType       | Тип используемого оборудования для хранилища (возможные значения – HDD или SSD)                                                                                                                                                                                                                                                                                               | HDD                   |
| PgLogLevel           | Уровень журналирования работы СУБД PostgreSQL (возможные значения – panic, fatal, log, error, warning, notice, info, debug1, debug2, debug3, debug4 или debug5)                                                                                                                                                                                                               | warning               |
| PgPassword           | Пароль служебной учетной записи для доступа к СУБД PostgreSQL                                                                                                                                                                                                                                                                                                                 | P@ssw0rdP@ssw0rd      |
| PgPort               | Порт для доступа к СУБД PostgreSQL                                                                                                                                                                                                                                                                                                                                            | 5432                  |
| PgSharedBufferSize   | Объем памяти, который будет использовать сервер баз данных для буферов в разделяемой памяти                                                                                                                                                                                                                                                                                   | 4GB                   |
| PgUser               | Логин служебной учетной записи для доступа к СУБД PostgreSQL                                                                                                                                                                                                                                                                                                                  | pt_system             |
| PgVacuumNapTime      | Минимальная задержка между двумя запусками автоочистки для отдельной базы данных                                                                                                                                                                                                                                                                                              | 20min                 |
| PgWorkMem            | Объем памяти, который будет использоваться для внутренних операций сортировки и хеш-таблиц, прежде чем будут задействованы временные файлы на диске                                                                                                                                                                                                                           | 200MB                 |

| Параметр                                         | Описание                                                                                                                                                        | Значение по умолчанию                       |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|
| SSLCertificatePemFileName                        | Имя файла сертификата SSL в формате PEM                                                                                                                         | Portal.crt                                  |
| SSLKeyFileName                                   | Имя файла закрытого ключа SSL-сертификата                                                                                                                       | Portal.key                                  |
| <b>Параметры конфигурации роли JatobaStorage</b> |                                                                                                                                                                 |                                             |
| CACertificateFileName                            | Имя файла корневого сертификата                                                                                                                                 | rootCA.crt                                  |
| CollectorAgentHttpPort                           | Порт для доступа к коллектору OpenTelemetry в роли SqlStorage/JatobaStorage по протоколу HTTP                                                                   | 4319                                        |
| CollectorAgentSyslogUdpPort                      | Порт для прослушивания журналов syslog по протоколу UDP                                                                                                         | 54528                                       |
| DockerRegistry                                   | Порт для доступа к реестру Docker-образов                                                                                                                       | Адрес сервера компонента Ankey SIEM NG Core |
| EnableFilesLogCollection                         | Запись журналов в файл вместо их централизованного сбора включена (True) или выключена (False)                                                                  | False                                       |
| HostAddress                                      | IP-адрес или FQDN сервера с установленной ролью SqlStorage/JatobaStorage                                                                                        | —                                           |
| Network                                          | Сетевое имя реестра Docker-образов                                                                                                                              | storage-network.sqlstorage                  |
| NetworkDriver                                    | Драйвер Docker-образов                                                                                                                                          | bridge                                      |
| PgAdminPort                                      | Порт для доступа к PgAdmin                                                                                                                                      | 9001                                        |
| PgEffectiveCacheSize                             | Эффективный размер дискового кэша, доступный для одного запроса                                                                                                 | 6GB                                         |
| PgEmail                                          | Электронный адрес служебной учетной записи для доступа к СУБД PostgreSQL                                                                                        | email@email.com                             |
| PgHardDiskType                                   | Тип используемого оборудования для хранилища (возможные значения – HDD или SSD)                                                                                 | HDD                                         |
| PgLogLevel                                       | Уровень журналирования работы СУБД PostgreSQL (возможные значения – panic, fatal, log, error, warning, notice, info, debug1, debug2, debug3, debug4 или debug5) | warning                                     |
| PgPassword                                       | Пароль служебной учетной записи для доступа к СУБД PostgreSQL                                                                                                   | P@ssw0rdP@ssw0rd                            |
| PgPort                                           | Порт для доступа к СУБД PostgreSQL                                                                                                                              | 5432                                        |
| PgSharedBufferSize                               | Объем памяти, который будет использовать сервер баз данных для буферов в разделяемой памяти                                                                     | 4GB                                         |

| Параметр                  | Описание                                                                                                                                            | Значение по умолчанию |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| PgUser                    | Логин служебной учетной записи для доступа к СУБД PostgreSQL                                                                                        | pt_system             |
| PgWorkMem                 | Объем памяти, который будет использоваться для внутренних операций сортировки и хеш-таблиц, прежде чем будут задействованы временные файлы на диске | 200MB                 |
| SSLCertificatePemFileName | Имя файла сертификата SSL в формате PEM                                                                                                             | Portal.crt            |
| SSLKeyFileName            | Имя файла закрытого ключа SSL-сертификата                                                                                                           | Portal.key            |

Таблица Б.3 – Параметры конфигурации роли Management and Configuration

| Параметр                   | Описание                                                                                                                                                             | Значение по умолчанию |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| ActionLogBatchSize         | Количество записей о действиях пользователей, которые служба MC Identity and Access Management Service одновременно отправляет службе MC User Action Logging Service | 100                   |
| ActionLogMillisecondsDelay | Тайм-аут между попытками отправки записей о действиях пользователей (в миллисекундах)                                                                                | 1000                  |
| DefaultLocale              | Интерфейс Ankey SIEM NG MC отображается на русском (ru-RU) или английском (en-US) языке                                                                              | ru-Ru                 |
| ExpertDataUpdateMethod     | Метод получения обновлений экспертных данных. Возможные значения: Online или Offline                                                                                 | –                     |
| HostAddress                | IP-адрес или FQDN сервера Ankey SIEM NG MC                                                                                                                           | –                     |
| IamCookieLifetime          | Время жизни неактивной сессии в Ankey SIEM NG с компонентом Ankey SIEM NG VM (в часах)                                                                               | 168                   |
| LdapTimeout                | Тайм-аут подключения к LDAP-серверу (в миллисекундах)                                                                                                                | 60000                 |
| LogCleanLimit              | Максимальное количество сохраняемых записей о действиях пользователей. При превышении заданного значения старые записи будут удалены                                 | 1000000               |
| MasterRedirectEnabled      | В случае иерархической установки аутентификация пользователя выполняется на главной (флажок установлен) или на локальной (флажок снят) площадке                      | Флажок снят           |
| PackageManagementPort      | Номер порта сервиса управления пакетами Package Management                                                                                                           | 8585                  |

| Параметр                      | Описание                                                                                                                                                                      | Значение по умолчанию |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| PackagesSourceCredentialToken | Токен для авторизации на сервере обновлений. Хранится в файле instance-access-token.key и представляет собой набор символов, закодированных с использованием стандарта Base64 | –                     |
| PackagesSourceUri             | Адрес сервера обновлений                                                                                                                                                      | –                     |
| PostgreHost                   | IP-адрес или FQDN сервера с установленной ролью SqlStorage/JatobaStorage                                                                                                      | –                     |
| PostgrePassword               | Пароль служебной учетной записи для доступа Ankey SIEM NG MC к СУБД PostgreSQL                                                                                                | P@ssw0rdP@ssw0rd      |
| PostgrePort                   | Порт сервера СУБД PostgreSQL для входящих подключений от Ankey SIEM NG MC                                                                                                     | 5432                  |
| PostgreUserName               | Логин служебной учетной записи для доступа Ankey SIEM NG MC к СУБД PostgreSQL                                                                                                 | pt_system             |
| TmSiteAlias                   | Псевдоним площадки                                                                                                                                                            | SITE                  |
| TmSiteId                      | Идентификатор площадки                                                                                                                                                        | –                     |
| TmTenantManagerId             | Идентификатор службы MC Tenant Manager Service                                                                                                                                | –                     |

Таблица Б.4 – Параметры конфигурации роли Knowledge Base

| Параметр                | Описание                                                                                                                      | Значение по умолчанию |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| ClientId                | Идентификатор для регистрации приложения Knowledge Base в Ankey SIEM NG MC                                                    | ptkb                  |
| ClientSecret            | Ключ для регистрации приложения Knowledge Base в Ankey SIEM NG MC                                                             | secret                |
| CoreAddress             | IP-адрес или FQDN сервера Ankey SIEM NG Core                                                                                  | localhost             |
| DefaultLocale           | Интерфейс Knowledge Base отображается на русском (ru-RU) или английском (en-US) языке                                         | –                     |
| DeploymentType          | Тип развертывания Knowledge Base                                                                                              | –                     |
| DetectOutOfSyncWithSIEM | Knowledge Base определяет (флажок установлен) или не определяет (флажок снят) отсутствие синхронизации с Ankey SIEM NG Server | Флажок установлен     |

| Параметр          | Описание                                                                                                                                                 | Значение по умолчанию |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| DisplayName       | Название приложения Knowledge Base в Ankey SIEM NG MC                                                                                                    | Knowledge Base        |
| EditableOrigins   | Поставщик, атрибуты объектов которого можно изменять                                                                                                     | Local                 |
| HostAddress       | IP-адрес или FQDN сервера Knowledge Base                                                                                                                 | localhost             |
| MCAddress         | IP-адрес или FQDN сервера Ankey SIEM NG MC                                                                                                               | –                     |
| OriginNameENG     | Полное название поставщика для объектов Knowledge Base на английском языке                                                                               | Local system          |
| OriginNameRUS     | Полное название поставщика для объектов Knowledge Base на русском языке                                                                                  | Локальная система     |
| OriginNickName    | Псевдоним поставщика для объектов Knowledge Base                                                                                                         | LOC                   |
| OriginSystemName  | Поставщик объектов Knowledge Base                                                                                                                        | Local                 |
| PostgreHost       | IP-адрес или FQDN сервера БД PostgreSQL                                                                                                                  | localhost             |
| PostgrePassword   | Пароль служебной учетной записи для подключения Knowledge Base к СУБД PostgreSQL                                                                         | P@ssw0rdP@ssw0rd      |
| PostgrePort       | Порт сервера СУБД PostgreSQL для входящих подключений от Knowledge Base                                                                                  | 5432                  |
| PostgreUserName   | Логин служебной учетной записи для подключения Knowledge Base к СУБД PostgreSQL                                                                          | pt_system             |
| RestrictedLocales | Не используемый в Knowledge Base язык локализации                                                                                                        | KOR                   |
| ShowDiffObjectId  | Веб-интерфейс Knowledge Base отображает (флажок установлен) или не отображает (флажок снят) идентификаторы объектов (например, при сравнении ревизий БД) | Флажок снят           |

| Параметр                   | Описание                                                                                                                                                                                                                                                                                                                           | Значение по умолчанию                                             |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| Smtphost                   | IP-адрес или FQDN SMTP-сервера                                                                                                                                                                                                                                                                                                     | localhost                                                         |
| Smtppassword               | Пароль служебной учетной записи для подключения Knowledge Base к SMTP-серверу                                                                                                                                                                                                                                                      | –                                                                 |
| Smtpport                   | Порт SMTP-сервера для входящих подключений от Knowledge Base                                                                                                                                                                                                                                                                       | 25                                                                |
| Smtpsender                 | Значение поля «Отправитель» в уведомлении, отправляемом по электронной почте                                                                                                                                                                                                                                                       | Knowledge Base Notification System<br><NoReply@knowledgebase.com> |
| SmtptUseDefaultCredentials | Режим аутентификации SMTP-сервера: флажок установлен – для аутентификации используются логин и пароль служебной учетной записи Network Service (необходимо очистить значения параметров SmtptUser и SmtptPassword); флажок снят – для аутентификации используются логин и пароль, указанные в параметрах SmtptUser и SmtptPassword | Флажок установлен                                                 |
| SmtptUser                  | Логин служебной учетной записи для подключения Knowledge Base к SMTP-серверу                                                                                                                                                                                                                                                       | –                                                                 |

Таблица Б.5 – Параметры конфигурации роли Core

| Параметр                 | Описание                                                                                                                         | Значение по умолчанию |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| ConsiderEventsImportance | В случае изменения IP-адреса актива система обновляет его конфигурацию сразу (флажок установлен) или по расписанию (флажок снят) | Флажок установлен     |
| ContentDeployerPort      | Номер порта сервиса установки обновлений экспертизы Content Deployer                                                             | 8586                  |
| DefaultAssetTtl          | Время устаревания активов (<Дни>.<Часы>.<Минуты>.<Секунды>)                                                                      | 90.00:00:00           |
| DefaultLocale            | Интерфейс Ankey SIEM NG с компонентом Ankey SIEM NG VM отображается на русском (ru-RU) или английском (en-US) языке              | ru-RU                 |

| Параметр                            | Описание                                                                                                                                 | Значение по умолчанию |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| EmailNotificationRetryCount         | Максимальное количество попыток отправки сообщения на SMTP-сервер                                                                        | 10                    |
| EmailNotificationRetryPeriodSeconds | Период между попытками отправки сообщения на SMTP-сервер (в секундах)                                                                    | 60                    |
| HostAddress                         | IP-адрес или FQDN сервера Ankey SIEM NG Core                                                                                             | localhost             |
| IncidentAggregationTimeout          | Период, в течение которого срабатывания одного и того же правила корреляции агрегируются в один автоинцидент (<Часы>:<Минуты>:<Секунды>) | 00:01:00              |
| IncidentIdenticalNotificationLimit  | Максимальное количество срабатываний правила корреляции, которые могут агрегироваться в один инцидент                                    | 100                   |
| KBAddress                           | IP-адрес или FQDN сервера Knowledge Base                                                                                                 | –                     |
| MCAddress                           | IP-адрес или FQDN сервера Ankey SIEM NG MC                                                                                               | –                     |
| PostgreHost                         | IP-адрес или FQDN сервера СУБД PostgreSQL                                                                                                | localhost             |
| PostgrePassword                     | Пароль служебной учетной записи для подключения Ankey SIEM NG Core к СУБД PostgreSQL                                                     | P@ssw0rdP@ssw0rd      |
| PostgrePort                         | Порт сервера СУБД PostgreSQL для входящих подключений от Ankey SIEM NG Core                                                              | –                     |
| PostgreUserName                     | Логин служебной учетной записи для подключения Ankey SIEM NG Core к СУБД PostgreSQL                                                      | pt_system             |
| PtkbDbName                          | Имя базы знаний, из которой импортируются данные об уязвимостях                                                                          | –                     |
| PtkbUpdateCheckPeriod               | Период проверки наличия обновления для базы знаний, используемой в Ankey SIEM NG Core (<Часы>:<Минуты>:<Секунды>)                        | 00:05:00              |
| RMQHost                             | IP-адрес или FQDN сервера RabbitMQ                                                                                                       | localhost             |
| RMQPassword                         | Пароль служебной учетной записи для подключения Ankey SIEM NG Core к RabbitMQ                                                            | P@ssw0rd              |
| RMQSslServerName                    | IP-адрес или FQDN SSL-сервера RabbitMQ                                                                                                   | localhost             |
| RMQUser                             | Логин служебной учетной записи для подключения Ankey SIEM NG Core к RabbitMQ                                                             | mpx_core              |
| SiemFrontendAddress                 | IP-адрес или FQDN сервера Ankey SIEM NG Server                                                                                           | –                     |
| SendAlertsToSiem                    | При нарушении и восстановлении контролируемых параметров источников регистрируются соответствующие события (флажок)                      | Флажок не установлен  |

| Параметр                        | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Значение по умолчанию                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
|                                 | установлен). Если флажок не установлен, события не регистрируются                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                        |
| SmtpHost                        | IP-адрес или FQDN SMTP-сервера                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | localhost                                              |
| SmtpIgnoreCertificateValidation | Ankey SIEM NG Core проверяет (False) или не проверяет (True) валидность сертификата при подключении к SMTP-серверу                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | True                                                   |
| SmtpPassword                    | Пароль служебной учетной записи для подключения Ankey SIEM NG Core к SMTP-серверу                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | –                                                      |
| SmtpPort                        | Порт SMTP-сервера для входящих подключений от Ankey SIEM NG Core                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 25                                                     |
| SmtpSecureSocketOptions         | Варианты шифрования при подключении к SMTP-серверу:<br>None – шифрование не используется;<br>Auto – почтовый сервер определяет, использовать ли протокол SSL или протокол TLS. Если сервер не поддерживает протоколы SSL и TLS, то шифрование не используется;<br>SslOnConnect – протоколы SSL или TLS используются при соединении;<br>StartTls – протокол TLS используется после приветствия сервера. Если сервер не поддерживает расширение STARTTLS, соединение прерывается;<br>StartTlsWhenAvailable – протокол TLS используется после приветствия сервера, если сервер поддерживает расширение STARTTLS | Auto                                                   |
| SmtpSender                      | Значение поля «Отправитель» в уведомлении, отправляемом по электронной почте                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Notification System<br><NoReply@SiemNotifications.com> |
| SmtpUser                        | Логин служебной учетной записи для подключения Ankey SIEM NG Core к SMTP-серверу                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | –                                                      |
| TtlCheckPeriod                  | Период проверки (<Дни>.<Часы>:<Минуты>:<Секунды>) состояния актива (устарел актив или нет)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 01.00:00:00                                            |
| UsageMonitoringCheckingPeriod   | Период запуска проверок по чек-листу (<Часы>:<Минуты>:<Секунды>)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 00:15:00                                               |
| UsePtbkServer                   | Ankey SIEM NG Core проверяет (флажок установлен) или не проверяет (флажок снят) наличие обновления базы знаний об уязвимостях в Knowledge Base                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Флажок установлен                                      |

| Параметр                      | Описание                                                                                                                           | Значение по умолчанию |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| VulnerStateCheckInterval      | Период проверки статусов экземпляров уязвимостей (<Дни>.<Часы>:<Минуты>:<Секунды>)                                                 | 01.00:00:00           |
| VulnerStateCheckPeriodEnabled | Ankey SIEM NG Core проверяет (флажок установлен) или не проверяет (флажок снят) статусы экземпляров уязвимостей                    | Флажок установлен     |
| VulnerStateCheckPeriodEnd     | Время окончания суточного периода, в котором может запускаться проверка (от 00:00:00 до 23:59:59)                                  | 01:00:00              |
| VulnerStateCheckPeriodOfRetry | Продолжительность паузы (<Часы>:<Минуты>:<Секунды>) перед повторным запуском проверки, если предыдущий запуск завершился с ошибкой | 00:01:00              |
| VulnerStateCheckPeriodStart   | Время начала суточного периода, в котором может запускаться проверка (от 00:00:00 до 23:59:59)                                     | 00:00:00              |

Таблица Б.6 – Параметры конфигурации роли Collector

| Параметр                        | Описание                                                                                                                                                                   | Значение по умолчанию |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| AgentMonitoringCacheAlarm       | Пороговое значение для объема свободного места на всех логических дисках с файлами коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2    | –                     |
| AgentMonitoringCacheWarn        | Пороговое значение для объема свободного места на всех логических дисках с файлами коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1    | –                     |
| AgentMonitoringDiskLogsAlarm    | Пороговое значение для объема свободного места на логическом диске с файлами журналов коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2 | –                     |
| AgentMonitoringDiskLogsWarn     | Пороговое значение для объема свободного места на логическом диске с файлами журналов коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1 | –                     |
| AgentMonitoringDiskOverallAlarm | Пороговое значение для параметров AgentMonitoringDiskLogsAlarm, AgentMonitoringDiskStorageAlarm, AgentMonitoringDiskQueueAlarm (групповое указание значений)               | 32768M free           |
| AgentMonitoringDiskOverallWarn  | Пороговое значение для параметров AgentMonitoringDiskLogsWarn, AgentMonitoringDiskStorageWarn, AgentMonitoringDiskQueueWarn (групповое указание значений)                  | –                     |

| Параметр                        | Описание                                                                                                                                                                                                                                                                                                                                                                              | Значение по умолчанию                |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| AgentMonitoringDiskQueueAlarm   | Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения коллектор переходит в режим SafeMode2                                                                                                                                                                                                                | —                                    |
| AgentMonitoringDiskQueueWarn    | Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения коллектор переходит в режим SafeMode1                                                                                                                                                                                                                | —                                    |
| AgentMonitoringDiskStorageAlarm | Пороговое значение для объема свободного места на логическом диске с файлами базы данных коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2                                                                                                                                                                                                         | —                                    |
| AgentMonitoringDiskStorageWarn  | Пороговое значение для объема свободного места на логическом диске с файлами базы данных коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1                                                                                                                                                                                                         | —                                    |
| AgentName                       | Имя коллектора в веб-интерфейсе Ankey SIEM NG с компонентом Ankey SIEM NG VM                                                                                                                                                                                                                                                                                                          | FQDN сервера Ankey SIEM NG Collector |
| AgentRMQHost                    | IP-адрес или FQDN сервера RabbitMQ.<br><b>Примечание.</b> Брокер RabbitMQ обеспечивает обмен сообщениями между компонентами Ankey SIEM NG с компонентом Ankey SIEM NG VM. Брокер устанавливается на сервер Ankey SIEM NG Core в конфигурации для низконагруженных систем и на сервера Ankey SIEM NG Core и Ankey SIEM NG Server в конфигурации для средне- и высоконагруженных систем | localhost                            |
| AgentRMQPassword                | Пароль служебной учетной записи для подключения Ankey SIEM NG Collector к RabbitMQ                                                                                                                                                                                                                                                                                                    | P@ssw0rd                             |
| AgentRMQPort                    | Порт сервера RabbitMQ для входящих подключений от Ankey SIEM NG Collector                                                                                                                                                                                                                                                                                                             | 5671                                 |
| AgentRMQUser                    | Логин служебной учетной записи для подключения Ankey SIEM NG Collector к RabbitMQ                                                                                                                                                                                                                                                                                                     | agent                                |
| AgentRMQVirtualHost             | Имя виртуального узла RabbitMQ                                                                                                                                                                                                                                                                                                                                                        | mpx                                  |
| Agent_RMQ_SSL_CA_Certificate    | Путь к файлу корневого SSL-сертификата                                                                                                                                                                                                                                                                                                                                                | RMQ_Server.crt                       |

Таблица Б.7 – Параметры конфигурации роли SIEM Storage

| Параметр                    | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Значение по умолчанию |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| BindHost                    | IP-адреса или FQDN сетевых интерфейсов сервера Ankey SIEM NG Events Storage.<br><b>Примечание.</b> Elasticsearch обрабатывает входящие запросы, поступающие только на эти сетевые интерфейсы                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 0.0.0.0               |
| ClientNodeHeapSize          | Объем оперативной памяти, выделяемый для клиентского узла (в гигабайтах).<br><b>Примечание.</b> Перед изменением параметра необходимо выбрать вариант Manual в качестве значения параметра ClusterConfigurationProfile                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 16g                   |
| ClusterConfigurationProfile | Объем оперативной памяти, выделяемый каждому типу узлов кластера Elasticsearch. Для выбора доступны следующие варианты:<br>AIO – значения установлены производителем и соответствуют требованиям конфигурации Ankey SIEM NG с компонентом Ankey SIEM NG VM для низконагруженных систем;<br>SIEMandStorage – значения установлены производителем и соответствуют требованиям конфигурации Ankey SIEM NG с компонентом Ankey SIEM NG VM для средненагруженных систем;<br>Standalone – значения установлены производителем и соответствуют требованиям конфигурации Ankey SIEM NG с компонентом Ankey SIEM NG VM для высоконагруженных систем с потоком событий до 20000 в секунду;<br>ManagedStorage – значения установлены производителем и соответствуют требованиям конфигурации Ankey SIEM NG с компонентом Ankey SIEM NG VM для высоконагруженных систем с потоком событий выше 20000 в секунду;<br>Manual – ввод значений вручную (параметры DataNodeHeapSize, ClientNodeHeapSize, MasterNodeHeapSize) | Standalone            |
| DataNodeHeapSize            | Объем оперативной памяти, выделяемый для одного узла данных (в гигабайтах).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 30g                   |

| Параметр           | Описание                                                                                                                                                                                                            | Значение по умолчанию           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
|                    | <b>Примечание.</b> Перед изменением параметра необходимо выбрать вариант Manual в качестве значения параметра ClusterConfigurationProfile                                                                           |                                 |
| HighLoad           | Кластер Elasticsearch содержит два (флажок снят) или четыре (флажок установлен) узла данных                                                                                                                         | Флажок снят                     |
| HostAddress        | IP-адрес или FQDN сервера Ankey SIEM NG Events Storage                                                                                                                                                              | —                               |
| MasterNodeHeapSize | Объем оперативной памяти, выделяемый для главного узла (в гигабайтах).<br><b>Примечание.</b> Перед изменением параметра необходимо выбрать вариант Manual в качестве значения параметра ClusterConfigurationProfile | 16g                             |
| PathData           | Путь к индексам Elasticsearch. Если Ankey SIEM NG с компонентом Ankey SIEM NG VM развернут для высоконагруженных систем – путь к индексам, находящимся в теплой стадии                                              | /data                           |
| PathDataHot        | Путь к индексам, находящимся в горячей стадии                                                                                                                                                                       | /datahot                        |
| PathLog            | Путь к файлам журналов                                                                                                                                                                                              | /es_logs                        |
| PathRepo           | Путь к резервным копиям индексов                                                                                                                                                                                    | /es_backup                      |
| RotateCount        | Максимальное количество файлов журналов для компонентов сторонних производителей                                                                                                                                    | 10                              |
| RotateSize         | Максимальный размер файла журнала для компонентов сторонних производителей (G для гигабайтов, M для мегабайтов, k для килобайтов)                                                                                   | 200M                            |
| TailcutterDbSpace  | Максимальный объем дискового пространства, выделяемый для хранения индексов, в гигабайтах (например, 1000) или процентах от общего объема жесткого диска (например, 65%)                                            | 92%                             |
| TailcutterLog      | Путь к файлу журнала утилиты tailcutter                                                                                                                                                                             | /opt/estools/log/tailcutter.log |
| TailcutterLogLevel | Уровень журналирования работы утилиты tailcutter (возможные значения CRITICAL, ERROR, WARNING, INFO, DEBUG и NOTSET)                                                                                                | WARNING                         |
| TailcutterTtl      | Срок хранения индексов для событий (в днях)                                                                                                                                                                         | 365                             |
| TailcutterTtlc     | Срок хранения индексов для счетчиков событий (в днях)                                                                                                                                                               | 7                               |

Таблица Б.8 – Параметры конфигурации роли SIEM Server

| Параметр                              | Описание                                                                                                                                                                                                                                                                                                                            | Значение по умолчанию     |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| AssetResolverPort                     | Порт сервера Ankey SIEM NG Core для подключения службы SIEM Server assets resolution                                                                                                                                                                                                                                                | 8721                      |
| AUTH_KEY                              | Путь к файлу закрытого ключа сертификата для аутентификации Ankey SIEM NG Server в Ankey SIEM NG MC                                                                                                                                                                                                                                 | /opt/siem/etc/authKey.pem |
| ClusterSeedHost                       | IP-адрес или FQDN сервера Ankey SIEM NG Events Storage для входящих подключений от связанных приложений при выполнении распределенного поиска событий                                                                                                                                                                               | –                         |
| ClusterSeedPort                       | Порт сервера Ankey SIEM NG Events Storage для входящих подключений от связанных приложений при выполнении распределенного поиска событий                                                                                                                                                                                            | 9300                      |
| CoreAddress                           | IP-адрес или FQDN сервера Ankey SIEM NG Core                                                                                                                                                                                                                                                                                        | localhost                 |
| CorePort                              | Порт сервера Ankey SIEM NG Core для подключения Ankey SIEM NG Server                                                                                                                                                                                                                                                                | 8799                      |
| CoreRabbitAuthMethod                  | Аутентификация Ankey SIEM NG Server в брокере RabbitMQ выполняется с помощью логина и пароля (plain) или с помощью сертификатов безопасности (ssl).<br><b>Примечание.</b> Этот брокер устанавливается на сервер Ankey SIEM NG Core и обеспечивает обмен сообщениями между компонентами Ankey SIEM NG с компонентом Ankey SIEM NG VM | ssl                       |
| CoreTableListsSize                    | Объем оперативной памяти для хранения табличных списков, заполняемых правилами корреляции (в мегабайтах)                                                                                                                                                                                                                            | 16384                     |
| CorrTableListsSize                    | Объем оперативной памяти для хранения табличных списков, заполняемых данными об активах, справочной информацией и данными от репутационных сервисов (в мегабайтах)                                                                                                                                                                  | 4096                      |
| CounterRefreshInterval                | Период обновления данных о счетчиках производительности (в секундах)                                                                                                                                                                                                                                                                | 60                        |
| CsvSeparator                          | Разделитель данных в CSV-файле, используемом для экспорта и импорта табличных списков                                                                                                                                                                                                                                               | ;                         |
| DefaultLogLevel                       | Уровень журналирования для служб Ankey SIEM NG Server (возможные значения – fatal, error, warn, info, debug или trace)                                                                                                                                                                                                              | info                      |
| ElasticsearchAggregationQueryTime out | Тайм-аут для поиска событий, подходящих под условия группировки или агрегации (в секундах)                                                                                                                                                                                                                                          | 600                       |

| Параметр                                | Описание                                                                                                                                                                                                                                                    | Значение по умолчанию |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| ElasticsearchAggregationResponseTimeout | Тайм-аут выполнения запроса группировки или агрегации событий (в секундах)                                                                                                                                                                                  | 600                   |
| ElasticsearchAggregationSize            | Максимальное количество групп, отображаемое в результате группировки или агрегации событий                                                                                                                                                                  | 1000                  |
| ElasticsearchAPIVersion                 | Версия API, используемая для взаимодействия с Elasticsearch                                                                                                                                                                                                 | 7.4                   |
| ElasticsearchCompression                | Алгоритм сжатия данных, используемый в Elasticsearch                                                                                                                                                                                                        | default               |
| ElasticsearchCountersLimit              | Максимальное количество записей о счетчиках производительности, получаемых от Elasticsearch (0 – количество получаемых записей не ограничено)                                                                                                               | 0                     |
| ElasticsearchDefaultQueryTimeout        | Тайм-аут для поиска событий, подходящих под условия фильтрации (в секундах)                                                                                                                                                                                 | 600                   |
| ElasticsearchDefaultResponseTimeout     | Тайм-аут выполнения запроса фильтрации событий (в секундах)                                                                                                                                                                                                 | 600                   |
| ElasticsearchHost                       | IP-адрес или FQDN сервера Ankey SIEM NG Events Storage                                                                                                                                                                                                      | localhost             |
| ElasticsearchMaxReplySize               | Максимальный размер ответа от Elasticsearch (в байтах)                                                                                                                                                                                                      | 524288000             |
| EnriTableListsSize                      | Объем оперативной памяти для хранения табличных списков, заполняемых правилами обогащения (в мегабайтах)                                                                                                                                                    | 8192                  |
| EventsCaseSensitiveSearch               | Тип поиска по схеме полей событий: регистрозависимый (True) или регистронезависимый (False).<br><b>Примечание.</b> Тип поиска изменится в течение суток после изменения параметра и применится только для тех событий, которые поступят после его изменения | False                 |
| EventsRefreshInterval                   | Период обновления данных о событиях (в секундах)                                                                                                                                                                                                            | 60                    |
| FrontendHost                            | IP-адрес для прослушивания службой SIEM Server frontend входящих подключений                                                                                                                                                                                | 0.0.0.0               |
| GlobalRabbitHost                        | IP-адрес или FQDN сервера RabbitMQ.<br><b>Примечание.</b> Этот брокер RabbitMQ устанавливается на сервер Ankey SIEM NG Server и обеспечивает обмен сообщениями между службами Ankey SIEM NG Server                                                          | 127.0.0.1             |
| GlobalRabbitPort                        | Порт сервера RabbitMQ для входящих соединений от Ankey SIEM NG Core                                                                                                                                                                                         | 5672                  |

| Параметр                       | Описание                                                                                                                                                                      | Значение по умолчанию |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| HighLoad                       | Для службы SIEM server storage выделено шесть (флажок установлен) или четыре (флажок снят) потока операционной системы                                                        | Флажок снят           |
| HostAddress                    | IP-адрес или FQDN Ankey SIEM NG Server                                                                                                                                        | –                     |
| LogCount                       | Максимальное количество файлов журналов Ankey SIEM NG Server (архивированных и неархивированных)                                                                              | 10                    |
| LogPlain                       | Максимальное количество неархивированных файлов журналов Ankey SIEM NG Server                                                                                                 | 2                     |
| LogSize                        | Максимальный размер файла журнала Ankey SIEM NG Server (в байтах)                                                                                                             | 104857600             |
| LogSpaceHost                   | IP-адрес или FQDN сервера Ankey SIEM NG Events Storage                                                                                                                        | localhost             |
| ManagedStorage                 | Для управления жизненным циклом индексов Elasticsearch используется (флажок установлен) или не используется (флажок снят) технология ILM                                      | Флажок снят           |
| MonitoringOomEnabled           | Мониторинг объема оперативной памяти, потребляемой правилами корреляции, выполняется (флажок установлен) или не выполняется (флажок снят)                                     | Флажок установлен     |
| MonitoringOomMemoryLimit       | Объем оперативной памяти, выделенный для работы правил корреляции (в гигабайтах)                                                                                              | 60                    |
| MonitoringOvertriggerEnabled   | Мониторинг количества корреляционных событий, регистрируемых правилами корреляции, выполняется (флажок установлен) или не выполняется (флажок снят)                           | Флажок установлен     |
| MonitoringOvertriggerPeriod    | Период для подсчета количества корреляционных событий, регистрируемых одним правилом корреляции (в секундах)                                                                  | 3600                  |
| MonitoringOvertriggerThreshold | Максимальное количество корреляционных событий за период (параметр MonitoringOvertriggerPeriod), регистрируемых одним правилом корреляции и не приводящее к остановке правила | 300                   |
| ProtectedRulesPath             | Путь к файлу со списком правил корреляции, работа которых приостанавливается в последнюю очередь (при мониторинге работы правил корреляции)                                   | –                     |
| RemoteEventsSkipAggregator     | Площадка-получатель выполняет (флажок снят) или не выполняет (флажок установлен) агрегацию реплицированных событий                                                            | Флажок установлен     |

| Параметр                   | Описание                                                                                                                                                                                                                     | Значение по умолчанию             |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| RemoteEventsSkipCorrelator | Площадка-получатель выполняет (флажок снят) или не выполняет (флажок установлен) корреляцию реплицированных событий                                                                                                          | Флажок установлен                 |
| RemoteEventsSkipEnricher   | Площадка-получатель выполняет (флажок снят) или не выполняет (флажок установлен) обогащение реплицированных событий                                                                                                          | Флажок установлен                 |
| RemoteEventsSkipResolver   | Площадка-получатель выполняет (флажок снят) или не выполняет (флажок установлен) привязку реплицированных событий к активам                                                                                                  | Флажок установлен                 |
| RMQ_SSL_CA_CERTIFICATE     | Путь к файлу корневого SSL-сертификата                                                                                                                                                                                       | /opt/siem/etc/rootCA.crt          |
| RMQ_SSL_CERTIFICATE        | Путь к файлу публичного SSL-сертификата                                                                                                                                                                                      | /opt/siem/etc/RMQ_SIEM_Client.crt |
| RMQ_SSL_KEY                | Путь к файлу закрытого ключа SSL-сертификата                                                                                                                                                                                 | /opt/siem/etc/RMQ_SIEM_Client.key |
| RMQDurableQueue            | Сообщения, накопленные в очередях RabbitMQ, сохраняются (флажок установлен) или не сохраняются (флажок снят) после перезагрузки брокера                                                                                      | Флажок установлен                 |
| RMQHost                    | IP-адрес или FQDN сервера RabbitMQ.<br><b>Примечание.</b> Этот брокер RabbitMQ устанавливается на сервер Ankey SIEM NG Core и обеспечивает обмен сообщениями между компонентами Ankey SIEM NG с компонентом Ankey SIEM NG VM | localhost                         |
| RMQPassword                | Пароль служебной учетной записи для подключения Ankey SIEM NG Server к брокеру RabbitMQ                                                                                                                                      | P@ssw0rd                          |
| RMQPort                    | Порт сервера RabbitMQ для входящих соединений от Ankey SIEM NG Server при аутентификации с помощью логина и пароля (plain)                                                                                                   | 5672                              |
| RMQPortSSL                 | Порт сервера RabbitMQ для входящих соединений от Ankey SIEM NG Server при аутентификации с помощью сертификатов безопасности (ssl)                                                                                           | 5671                              |
| RMQUser                    | Логин служебной учетной записи для подключения Ankey SIEM NG Server к брокеру RabbitMQ                                                                                                                                       | siem                              |

| Параметр                | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Значение по умолчанию |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| RowBatchSize            | Количество строк табличного списка, экспортируемых (импортируемых) службой SIEM Server frontend из службы (в службу) SIEM Server commander                                                                                                                                                                                                                                                                                                                                                                                           | 5000                  |
| SiemOnAgent             | Установлена облегченная (флажок установлен) или стандартная (флажок снят) версия Ankey SIEM NG Server                                                                                                                                                                                                                                                                                                                                                                                                                                | Флажок снят           |
| StatsPublishPeriod      | Период обновления данных, отображаемых в рабочей области главной страницы Ankey SIEM NG с компонентом Ankey SIEM NG VM (в секундах)                                                                                                                                                                                                                                                                                                                                                                                                  | 30                    |
| StorageBackendType      | В качестве хранилища событий используется Elasticsearch или LogSpace                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | elasticsearch         |
| StoreNormalizedRaw      | Нормализованные события сохраняются с полем body (флажок установлен) или без него (флажок снят)                                                                                                                                                                                                                                                                                                                                                                                                                                      | Флажок установлен     |
| StoreUnnormalizedRaw    | Ненормализованные события хранятся (флажок установлен) или не хранятся (флажок снят) в системе                                                                                                                                                                                                                                                                                                                                                                                                                                       | Флажок установлен     |
| TableListsRestorePolicy | Режим работы службы автоматического восстановления данных табличных списков SIEM Server fptarestor. Для выбора доступны следующие варианты:<br>disabled – автоматическое восстановление выключено;<br>fragile – данные будут восстановлены только в том случае, если при восстановлении исключена возможность их потери;<br>best_effort – в процессе восстановления допустима потеря одной-двух последних записей;<br>robust – в процессе восстановления допустима потеря всех данных (базы данных могут быть удалены и пересозданы) | best_effort           |
| WebProto                | HTTP-запросы к Ankey SIEM NG Core выполняются через защищенное (https) или незащищенное (http) соединение                                                                                                                                                                                                                                                                                                                                                                                                                            | https                 |

Таблица Б.9 – Параметры конфигурации роли RMQ Message Bus

| Параметр    | Описание                                                        | Значение по умолчанию |
|-------------|-----------------------------------------------------------------|-----------------------|
| CACertFile  | Имя файла корневого сертификата                                 | rootCA.crt            |
| CertFile    | Имя файла публичного сертификата                                | RMQ_Server.crt        |
| HostAddress | IP-адрес или FQDN сервера с установленной ролью RMQ Message Bus | –                     |
| KeyFile     | Имя файла закрытого ключа сертификата                           | RMQ_Server.pem        |

| Параметр                 | Описание                                                                                                                                                                                                                               | Значение по умолчанию |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| MEMORY_HIGH_WATERMARK_GB | Пороговое значение для объема оперативной памяти, потребляемой RabbitMQ (в гигабайтах).<br><b>Примечание.</b> Если объем оперативной памяти становится больше порогового значения, RabbitMQ останавливает прием входящих сообщений     | 10                    |
| RMQAdminPassword         | Пароль служебной учетной записи администратора RabbitMQ                                                                                                                                                                                | P@ssw0rd              |
| RMQAdminUser             | Логин служебной учетной записи администратора RabbitMQ                                                                                                                                                                                 | Administrator         |
| RMQAgentPassword         | Пароль служебной учетной записи для доступа коллекторов к RabbitMQ                                                                                                                                                                     | P@ssw0rd              |
| RMQAgentUser             | Логин служебной учетной записи для доступа коллекторов к RabbitMQ                                                                                                                                                                      | agent                 |
| RMQHttpPort              | Порт для доступа к RabbitMQ по протоколу HTTP                                                                                                                                                                                          | 5672                  |
| RMQHttpsPort             | Порт для доступа к RabbitMQ по протоколу HTTPS                                                                                                                                                                                         | 5671                  |
| RMQLogRotateSize         | Максимальный размер сохраняемых файлов журналов (G для гигабайтов, M для мегабайтов, k для килобайтов)                                                                                                                                 | 50M                   |
| RMQPassword              | Пароль служебной учетной записи для доступа Ankey SIEM NG Core к RabbitMQ                                                                                                                                                              | P@ssw0rd              |
| RMQSiemPassword          | Пароль служебной учетной записи для доступа Ankey SIEM NG Server к RabbitMQ                                                                                                                                                            | P@ssw0rd              |
| RMQSiemUser              | Логин служебной учетной записи для доступа Ankey SIEM NG Server к RabbitMQ                                                                                                                                                             | siem                  |
| RMQSslServerName         | IP-адрес или FQDN SSL-сервера RabbitMQ                                                                                                                                                                                                 | localhost             |
| RMQUser                  | Логин служебной учетной записи для доступа Ankey SIEM NG Core к RabbitMQ                                                                                                                                                               | core                  |
| RMQVirtualHost           | Имя виртуального узла RabbitMQ                                                                                                                                                                                                         | mpx                   |
| RMQ_DISK_FREE_LIMIT      | Пороговое значение для объема свободного места на логическом диске с RabbitMQ (в гигабайтах).<br><b>Примечание.</b> Если объем свободного места становится меньше порогового значения, RabbitMQ останавливает прием входящих сообщений | 20                    |
| WATERMARK_PAGING_RATIO   | Пороговое значение для объема оперативной памяти, потребляемой RabbitMQ (в доле от значения, указанного в MEMORY_HIGH_WATERMARK).                                                                                                      | 0.5                   |

| Параметр | Описание                                                                                                                                       | Значение по умолчанию |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
|          | <b>Примечание.</b> Если объем оперативной памяти становится больше порогового значения, RabbitMQ начинает сохранять входящие сообщения на диск |                       |

Таблица Б.10 – Параметры конфигурации роли Retro Correlator

| Параметр                        | Описание                                                                                                                                                                 | Значение по умолчанию |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| AgentMonitoringCacheAlarm       | Пороговое значение для объема свободного места на всех логических дисках с файлами коллктора. При достижении порогового значения коллктор переходит в режим SafeMode2    | –                     |
| AgentMonitoringCacheWarn        | Пороговое значение для объема свободного места на всех логических дисках с файлами коллктора. При достижении порогового значения коллктор переходит в режим SafeMode1    | –                     |
| AgentMonitoringDiskLogsAlarm    | Пороговое значение для объема свободного места на логическом диске с файлами журналов коллктора. При достижении порогового значения коллктор переходит в режим SafeMode2 | –                     |
| AgentMonitoringDiskLogsWarn     | Пороговое значение для объема свободного места на логическом диске с файлами журналов коллктора. При достижении порогового значения коллктор переходит в режим SafeMode1 | –                     |
| AgentMonitoringDiskOverallAlarm | Пороговое значение для параметров AgentMonitoringDiskLogsAlarm, AgentMonitoringDiskStorageAlarm, AgentMonitoringDiskQueueAlarm (групповое указание значений)             | 32768M free           |
| AgentMonitoringDiskOverallWarn  | Пороговое значение для параметров AgentMonitoringDiskLogsWarn, AgentMonitoringDiskStorageWarn, AgentMonitoringDiskQueueWarn (групповое указание значений)                | –                     |
| AgentMonitoringDiskQueueAlarm   | Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения коллктор переходит в режим SafeMode2    | –                     |
| AgentMonitoringDiskQueueWarn    | Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения коллктор переходит в режим SafeMode1    | –                     |
| AgentMonitoringDiskStorageAlarm | Пороговое значение для объема свободного места на логическом диске с файлами базы данных коллктора. При                                                                  | –                     |

| Параметр                       | Описание                                                                                                                                                                      | Значение по умолчанию         |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
|                                | достижении порогового значения коллектор переходит в режим SafeMode2                                                                                                          |                               |
| AgentMonitoringDiskStorageWarn | Пороговое значение для объема свободного места на логическом диске с файлами базы данных коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1 | —                             |
| AgentName                      | Имя коллектора в веб-интерфейсе Ankey SIEM NG с компонентом Ankey SIEM NG VM                                                                                                  | FQDN сервера Ankey SIEM NG RC |
| AgentRMQHost                   | IP-адрес или FQDN сервера RabbitMQ                                                                                                                                            | localhost                     |
| AgentRMQPassword               | Пароль служебной учетной записи для доступа Ankey SIEM NG RC к RabbitMQ                                                                                                       | P@ssw0rd                      |
| AgentRMQPort                   | Порт сервера RabbitMQ для входящих подключений от Ankey SIEM NG Collector                                                                                                     | 5671                          |
| AgentRMQUser                   | Логин служебной учетной записи для доступа Ankey SIEM NG RC к RabbitMQ                                                                                                        | agent                         |
| AgentRMQVirtualHost            | Имя виртуального узла RabbitMQ                                                                                                                                                | mpx                           |
| Agent_RMQ_SSL_CA_Certificate   | Путь к файлу корневого SSL-сертификата                                                                                                                                        | rootCA.crt                    |
| Agent_RMQ_SSL_Certificate      | Путь к файлу публичного SSL-сертификата                                                                                                                                       | RMQ_Agent_Client.crt          |
| Agent_RMQ_SSL_Enabled          | Ankey SIEM NG Collector подключается к RabbitMQ через защищенное (флажок установлен) или незащищенное (флажок снят) соединение                                                | Флажок установлен             |
| Agent_RMQ_SSL_Key              | Путь к файлу закрытого ключа SSL-сертификата                                                                                                                                  | RMQ_Agent_Client.key          |
| CoreAddress                    | IP-адрес или FQDN сервера Ankey SIEM NG Core                                                                                                                                  | localhost                     |
| CsvSeparator                   | Разделитель данных в CSV-файле, используемом для экспорта и импорта табличных списков                                                                                         | ;                             |
| DefaultLogLevel                | Уровень журналирования для служб Ankey SIEM NG RC (возможные значения – fatal, error, warn, info, debug или trace)                                                            | info                          |
| HostAddress                    | IP-адрес или FQDN сервера Ankey SIEM NG RC                                                                                                                                    | localhost                     |
| InternalRMQHost                | IP-адрес или FQDN сервера RabbitMQ                                                                                                                                            | localhost                     |
| InternalRMQPassword            | Пароль служебной учетной записи для доступа к RabbitMQ                                                                                                                        | P@ssw0rd                      |
| InternalRMQPort                | Порт сервера RabbitMQ для входящих соединений от Ankey SIEM NG RC при аутентификации с помощью логина и пароля (plain)                                                        | 5672                          |

| Параметр               | Описание                                                                                                                       | Значение по умолчанию |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| InternalRMQPortSSL     | Порт сервера RabbitMQ для входящих соединений от Ankey SIEM NG RC при аутентификации с помощью сертификатов безопасности (ssl) | 5671                  |
| InternalRMQUser        | Логин служебной учетной для доступа к RabbitMQ                                                                                 | siem                  |
| InternalRMQVirtualHost | Имя виртуального узла RabbitMQ                                                                                                 | /                     |
| KBAddress              | IP-адрес или FQDN сервера Knowledge Base                                                                                       | localhost             |
| LogCount               | Максимальное количество файлов журналов Ankey SIEM NG RC (архивированных и неархивированных)                                   | 10                    |
| LogPlain               | Максимальное количество неархивированных файлов журналов Ankey SIEM NG RC                                                      | 2                     |
| LogSize                | Максимальный размер файла журнала Ankey SIEM NG RC (в байтах)                                                                  | 104857600             |
| MaxTableListsSize      | Максимальный объем оперативной памяти, выделяемый для хранения табличных списков (в мегабайтах)                                | 8192                  |
| RetroControllerHost    | IP-адрес для входящих подключений от коллектора на Linux                                                                       | 0.0.0.0               |
| SiemServerAddress      | IP-адрес или FQDN сервера Ankey SIEM NG Server                                                                                 | localhost             |

## Приложение В

### Параметры конфигурации компонентов ПК Ankey SIEM NG на Microsoft Windows

Раздел содержит описание параметров конфигурации компонентов ПК Ankey SIEM NG на Microsoft Windows.

Таблица В.1 – Параметры конфигурации компонента Ankey SIEM NG Server

| Параметр             | Описание                                                                                                                                              | Значение по умолчанию                                                       |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| AUTH_KEY             | Путь к файлу закрытого ключа сертификата для аутентификации Ankey SIEM NG Server в Ankey SIEM NG MC                                                   | C:\ProgramData\Gazinformservice\Ankey SIEM NG Server\config\PKI\authKey.pem |
| ClusterSeedHost      | IP-адрес или FQDN сервера Ankey SIEM NG Events Storage для входящих подключений от связанных приложений при выполнении распределенного поиска событий | –                                                                           |
| ClusterSeedPort      | Порт сервера Ankey SIEM NG Events Storage для входящих подключений от связанных приложений при выполнении распределенного поиска событий              | 9300                                                                        |
| CoreAddress          | IP-адрес или FQDN сервера Ankey SIEM NG Core                                                                                                          | localhost                                                                   |
| CorePort             | Порт сервера Ankey SIEM NG Core для входящих подключений от Ankey SIEM NG Server                                                                      | 8799                                                                        |
| CoreRabbitAuthMethod | Аутентификация Ankey SIEM NG Server в RabbitMQ выполняется с помощью логина и пароля (plain) или с помощью сертификатов безопасности (ssl)            | ssl                                                                         |
| CoreTableListsSize   | Объем оперативной памяти для хранения табличных списков, заполняемых правилами корреляции (в мегабайтах)                                              | 16384                                                                       |
| CorrRegister         | Служба SIEM Server correlator запускается только после запуска службы SIEM Server commander (True) или независимо от ее запуска (False)               | True                                                                        |
| CorrTableListsSize   | Объем оперативной памяти для хранения табличных списков, заполняемых данными об                                                                       | 4096                                                                        |

| Параметр                                | Описание                                                                                                                                      | Значение по умолчанию |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
|                                         | активах, справочной информацией и данными от репутационных сервисов (в мегабайтах)                                                            |                       |
| CounterRefreshInterval                  | Период обновления данных о счетчиках производительности (в секундах)                                                                          | 60                    |
| CsvSeparator                            | Разделитель данных в CSV-файле, используемом для экспорта и импорта табличных списков                                                         | ;                     |
| DefaultLogLevel                         | Уровень журналирования для служб Ankey SIEM NG Server (возможные значения – fatal, error, warn, info, debug или trace)                        | info                  |
| ElasticsearchAggregationQueryTimeout    | Тайм-аут для поиска событий, подходящих под условия группировки или агрегации (в секундах)                                                    | 600                   |
| ElasticsearchAggregationResponseTimeout | Тайм-аут выполнения запроса группировки или агрегации событий (в секундах)                                                                    | 600                   |
| ElasticsearchAggregationSize            | Максимальное количество групп, отображаемое в результате группировки или агрегации событий                                                    | 1000                  |
| ElasticsearchAPIVersion                 | Версия API, используемая для взаимодействия с Elasticsearch                                                                                   | 7.4                   |
| ElasticsearchCompression                | Алгоритм сжатия данных, используемый в Elasticsearch                                                                                          | default               |
| ElasticsearchCountersLimit              | Максимальное количество записей о счетчиках производительности, получаемых от Elasticsearch (0 – количество получаемых записей не ограничено) | 0                     |
| ElasticsearchDefaultQueryTimeout        | Тайм-аут для поиска событий, подходящих под условия фильтрации (в секундах)                                                                   | 600                   |
| ElasticsearchDefaultResponseTimeout     | Тайм-аут выполнения запроса фильтрации событий (в секундах)                                                                                   | 600                   |
| ElasticsearchHost                       | IP-адрес или FQDN сервера Ankey SIEM NG Events Storage                                                                                        | localhost             |
| ElasticsearchMaxReplySize               | Максимальный размер ответа от Elasticsearch (в байтах)                                                                                        | 524288000             |
| EnriTableListsSize                      | Объем оперативной памяти для хранения табличных списков, заполняемых правилами обогащения (в мегабайтах)                                      | 8192                  |

| Параметр                  | Описание                                                                                                                                                                                                                                                                                | Значение по умолчанию |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| EnrRegister               | Служба SIEM Server enricher запускается только после запуска службы SIEM Server commander (True) или независимо от ее запуска (False)                                                                                                                                                   | True                  |
| EventsRefreshInterval     | Период обновления данных о событиях (в секундах)                                                                                                                                                                                                                                        | 60                    |
| EventsCaseSensitiveSearch | Тип поиска по схеме полей событий:<br>регистрозависимый (True) или регистронезависимый (False).<br><br><b>Примечание.</b> Тип поиска изменится в течение суток после изменения параметра и применится только для тех событий, которые поступят после его изменения                      | False                 |
| FrontendHost              | IP-адрес для прослушивания службой SIEM Server frontend входящих подключений                                                                                                                                                                                                            | 127.0.0.1             |
| GlobalRabbitHost          | IP-адрес или FQDN сервера RabbitMQ.<br><br><b>Примечание.</b> В конфигурации для низконагруженных систем брокер RabbitMQ устанавливается на сервер Ankey SIEM NG Core и обеспечивает обмен сообщениями между компонентами ПК Ankey SIEM NG, а также между службами Ankey SIEM NG Server | 127.0.0.1             |
| GlobalRabbitPort          | Порт сервера RabbitMQ для входящих подключений от Ankey SIEM NG Core                                                                                                                                                                                                                    | 5672                  |
| LogCount                  | Максимальное количество файлов журналов Ankey SIEM NG Server (архивированных и неархивированных)                                                                                                                                                                                        | 10                    |
| LogPlain                  | Максимальное количество неархивированных файлов журналов Ankey SIEM NG Server                                                                                                                                                                                                           | 2                     |
| LogSize                   | Максимальный размер файла журнала Ankey SIEM NG Server (в байтах)                                                                                                                                                                                                                       | 104857600             |
| MonitoringOomEnabled      | Мониторинг объема оперативной памяти, потребляемой правилами корреляции, выполняется (True) или не выполняется (False)                                                                                                                                                                  | True                  |

| Параметр                       | Описание                                                                                                                                                                      | Значение по умолчанию                                                                       |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| MonitoringOomMemoryLimit       | Объем оперативной памяти, выделенный для работы правил корреляции (в гигабайтах)                                                                                              | 60                                                                                          |
| MonitoringOvertriggerEnabled   | Мониторинг количества корреляционных событий, регистрируемых правилами корреляции, выполняется (True) или не выполняется (False)                                              | True                                                                                        |
| MonitoringOvertriggerPeriod    | Период для подсчета количества корреляционных событий, регистрируемых одним правилом корреляции (в секундах)                                                                  | 3600                                                                                        |
| MonitoringOvertriggerThreshold | Максимальное количество корреляционных событий за период (параметр MonitoringOvertriggerPeriod), регистрируемых одним правилом корреляции и не приводящее к остановке правила | 300                                                                                         |
| ProtectedRulesPath             | Путь к файлу со списком правил корреляции, работа которых приостанавливается в последнюю очередь (при мониторинге работы правил корреляции)                                   | –                                                                                           |
| RemoteEventsSkipAggregator     | Площадка-получатель выполняет (False) или не выполняет (True) агрегацию реплицированных событий                                                                               | True                                                                                        |
| RemoteEventsSkipCorrelator     | Площадка-получатель выполняет (False) или не выполняет (True) корреляцию реплицированных событий                                                                              | True                                                                                        |
| RemoteEventsSkipEnricher       | Площадка-получатель выполняет (False) или не выполняет (True) обогащение реплицированных событий                                                                              | True                                                                                        |
| RemoteEventsSkipResolver       | Площадка-получатель выполняет (False) или не выполняет (True) привязку реплицированных событий к активам                                                                      | True                                                                                        |
| RMQ_SSL_CA_CERTIFICATE         | Путь к файлу корневого SSL-сертификата                                                                                                                                        | C:\ProgramFiles\Gazinformservice\Ankey SIEMNGServer\install\scripts\Certificates\rootCA.crt |
| RMQ_SSL_CERTIFICATE            | Путь к файлу публичного SSL-сертификата                                                                                                                                       | C:\ProgramFiles\Gazinformservice\Ankey SIEM NGServer\install\scripts\Certificates           |

| Параметр        | Описание                                                                                                                                                                                                                                                                                | Значение по умолчанию                                                                                          |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
|                 |                                                                                                                                                                                                                                                                                         | \\RMQ_SIEM_Client.crt                                                                                          |
| RMQ_SSL_KEY     | Путь к файлу закрытого ключа SSL-сертификата                                                                                                                                                                                                                                            | C:\ProgramFiles\Gazinformservice\Ankey<br>SIEM NG Server\install\scripts\Certificates<br>\\RMQ_SIEM_Client.key |
| RMQDurableQueue | Сообщения, накопленные в очередях RabbitMQ, сохраняются (True) или не сохраняются (False) после перезагрузки брокера                                                                                                                                                                    | True                                                                                                           |
| RMQHost         | IP-адрес или FQDN сервера RabbitMQ.<br><br><b>Примечание.</b> В конфигурации для низконагруженных систем брокер RabbitMQ устанавливается на сервер Ankey SIEM NG Core и обеспечивает обмен сообщениями между компонентами ПК Ankey SIEM NG, а также между службами Ankey SIEM NG Server | localhost                                                                                                      |
| RMQPassword     | Пароль служебной учетной записи для подключения Ankey SIEM NG Server к RabbitMQ                                                                                                                                                                                                         | P@ssword                                                                                                       |
| RMQPort         | Порт сервера RabbitMQ для входящих подключений от Ankey SIEM NG Server при аутентификации с помощью логина и пароля (plain)                                                                                                                                                             | 5672                                                                                                           |
| RMQPortSSL      | Порт сервера RabbitMQ для входящих подключений от Ankey SIEM NG Server при аутентификации с помощью сертификатов безопасности (ssl)                                                                                                                                                     | 5671                                                                                                           |
| RMQUser         | Логин служебной учетной записи для подключения Ankey SIEM NG Server к RabbitMQ                                                                                                                                                                                                          | siem                                                                                                           |
| RMQVirtualHost  | Имя виртуального узла RabbitMQ для подключения Ankey SIEM NG Server                                                                                                                                                                                                                     | mpx                                                                                                            |
| RoutRegister    | Служба SIEM Server router запускается только после запуска службы SIEM Server commander (True) или независимо от ее запуска (False)                                                                                                                                                     | True                                                                                                           |
| RowBatchSize    | Количество строк табличного списка, экспортируемых (импортируемых) службой SIEM                                                                                                                                                                                                         | 5000                                                                                                           |

| Параметр                | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Значение по умолчанию                                                   |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
|                         | Server frontend из службы (в службу) SIEM Server commander                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                         |
| SiemOnAgent             | Установлена облегченная (True) или стандартная (False) версия Ankey SIEM NG Server                                                                                                                                                                                                                                                                                                                                                                                                                                                         | False                                                                   |
| StatsPublishPeriod      | Период обновления данных, отображаемых в рабочей области главной страницы ПК Ankey SIEM NG                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 30                                                                      |
| StoreNormalizedRaw      | Нормализованные события сохраняются с полем body (True) или без него (False)                                                                                                                                                                                                                                                                                                                                                                                                                                                               | True                                                                    |
| StoreUnnormalizedRaw    | Ненормализованные события хранятся (True) или не хранятся (False) в системе                                                                                                                                                                                                                                                                                                                                                                                                                                                                | True                                                                    |
| TableListsRestorePolicy | Режим работы службы автоматического восстановления данных табличных списков SIEM Server fptarestor. Вы можете указать следующие значения:<br>– disabled – автоматическое восстановление выключено;<br>– fragile – данные будут восстановлены только в том случае, если при восстановлении исключена возможность их потери;<br>– best_effort – в процессе восстановления допустима потеря одной-двух последних записей;<br>– robust – в процессе восстановления допустима потеря всех данных (базы данных могут быть удалены и пересозданы) | best_effort                                                             |
| TailcutterDbSpace       | Максимальный объем дискового пространства, выделяемый для хранения индексов, в гигабайтах (например, 1000) или процентах от общего объема жесткого диска (например, 65%)                                                                                                                                                                                                                                                                                                                                                                   | 92%                                                                     |
| TailcutterLog           | Путь к файлу журнала утилиты tailcutter                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | C:\ProgramData\Gazinformservice\Ankey SIEM NG Server\log\tailcutter.log |

| Параметр           | Описание                                                                                                             | Значение по умолчанию |
|--------------------|----------------------------------------------------------------------------------------------------------------------|-----------------------|
| TailcutterLogLevel | Уровень журналирования работы утилиты tailcutter (возможные значения CRITICAL, ERROR, WARNING, INFO, DEBUG и NOTSET) | WARNING               |
| TailcutterTtl      | Срок хранения индексов для событий (в днях)                                                                          | 365                   |
| TailcutterTtlc     | Срок хранения индексов для счетчиков событий (в днях)                                                                | 7                     |
| WebProto           | HTTP-запросы к Ankey SIEM NG Core выполняются через защищенное (https) или незащищенное (http) соединение            | https                 |

Таблица В.2 – Параметры конфигурации компонента Ankey SIEM NG Collector

| Параметр                        | Описание                                                                                                                                                                   | Значение по умолчанию |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| AgentMonitoringCacheAlarm       | Пороговое значение для объема свободного места на всех логических дисках с файлами коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2    | –                     |
| AgentMonitoringCacheWarn        | Пороговое значение для объема свободного места на всех логических дисках с файлами коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1    | –                     |
| AgentMonitoringDiskLogsAlarm    | Пороговое значение для объема свободного места на логическом диске с файлами журналов коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2 | –                     |
| AgentMonitoringDiskLogsWarn     | Пороговое значение для объема свободного места на логическом диске с файлами журналов коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1 | –                     |
| AgentMonitoringDiskOverallAlarm | Пороговое значение для параметров AgentMonitoringDiskLogsAlarm, AgentMonitoringDiskStorageAlarm, AgentMonitoringDiskQueueAlarm (групповое указание значений)               | 20480M free           |

| Параметр                        | Описание                                                                                                                                                                      | Значение по умолчанию                                                                                    |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| AgentMonitoringDiskOverallWarn  | Пороговое значение для параметров AgentMonitoringDiskLogsWarn, AgentMonitoringDiskStorageWarn, AgentMonitoringDiskQueueWarn (групповое указание значений)                     | –                                                                                                        |
| AgentMonitoringDiskQueueAlarm   | Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения коллектор переходит в режим SafeMode2        | –                                                                                                        |
| AgentMonitoringDiskQueueWarn    | Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения коллектор переходит в режим SafeMode1        | –                                                                                                        |
| AgentMonitoringDiskStorageAlarm | Пороговое значение для объема свободного места на логическом диске с файлами базы данных коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2 | –                                                                                                        |
| AgentMonitoringDiskStorageWarn  | Пороговое значение для объема свободного места на логическом диске с файлами базы данных коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1 | –                                                                                                        |
| AgentName                       | Имя коллектора в веб-интерфейсе ПК Ankey SIEM NG                                                                                                                              | FQDN сервера Ankey SIEM NG Collector                                                                     |
| RMQ_SSL_CA_CERTIFICATE          | Путь к файлу корневого SSL-сертификата                                                                                                                                        | C:\Program Files (x86)\Gazinformservice<br>Ankey SIEM NGAgent\install\scripts<br>Certificates\rootCA.crt |
| RMQ_SSL_CERTIFICATE             | Путь к файлу публичного SSL-сертификата                                                                                                                                       | C:\Program Files (x86)\Gazinformservice<br>Ankey SIEM NGAgent\install\scripts                            |

| Параметр       | Описание                                                                                                                                                                                    | Значение по умолчанию                                                                                                            |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
|                |                                                                                                                                                                                             | \\Certificates\\RMQ_Agent_Client.crt                                                                                             |
| RMQ_SSL_KEY    | Путь к файлу закрытого ключа SSL-сертификата                                                                                                                                                | C:\\Program Files(x86)\\Gazinformservice<br>\\Ankey SIEM NG Collector\\.install\\scripts<br>\\Certificates\\RMQ_Agent_Client.key |
| RMQHost        | IP-адрес или FQDN сервера RabbitMQ.<br><b>Примечание.</b> Брокер RabbitMQ устанавливается на сервер Ankey SIEM NG Core и обеспечивает обмен сообщениями между компонентами ПК Ankey SIEM NG | localhost                                                                                                                        |
| RMQPassword    | Пароль служебной учетной записи для подключения Ankey SIEM NG Collector к RabbitMQ                                                                                                          | P@ssword                                                                                                                         |
| RMQPort        | Порт сервера RabbitMQ для входящих подключений от Ankey SIEM NG Collector                                                                                                                   | 5671                                                                                                                             |
| RMQUser        | Логин служебной учетной записи для подключения Ankey SIEM NG Collector к RabbitMQ                                                                                                           | mpx_agent                                                                                                                        |
| RMQVirtualHost | Имя виртуального узла RabbitMQ                                                                                                                                                              | mpx                                                                                                                              |
| SSLEnabled     | Ankey SIEM NG Collector подключается к RabbitMQ через защищенное (True) или незащищенное (False) соединение                                                                                 | True                                                                                                                             |

## Приложение Г

### Рекомендуемые конфигурации для систем хранения событий информационной безопасности

Для размещения данных может использоваться одновременно несколько систем долговременного хранения. Рекомендуется разделить хранилище для событий в оперативном доступе от хранилища для архивных событий. Для обработки и хранения событий в оперативном доступе требуются высокопроизводительные твердотельные накопители. Для обработки и хранения архивных событий допустимо использовать менее производительные жесткие диски.

Для оперативного хранилища событий критичными параметрами являются:

- скорость операций случайной записи;
- скорость операций случайного чтения.

Для архивного хранилища событий критичным параметром является скорость операций последовательного чтения.

Поддерживаемые конфигурации при взаимодействии с внешними системами/устройствами хранения представлены в таблице Г.1.

Таблица Г.1 – Поддерживаемые конфигурации при взаимодействии с внешними системами/устройствами хранения

| Тип массивов данных                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Тип файловых систем для хранения | Тип жестких дисков                        | Возможные конфигурации и RAID | Рекомендуемый резерв дисков |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|-------------------------------------------|-------------------------------|-----------------------------|
| Direct Attached Storage;<br>Network Attached Storage;<br>Storage Area Network                                                                                                                                                                                                                                                                                                                                                                                                      | ext4                             | HDD (10000 об./мин.)/<br>(15000 об./мин.) | RAID 10<br>RAID 6***          | 1 Hot Spare**               |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                  | SSD*                                      | RAID 5<br>RAID 6<br>RAID 1    |                             |
| <p>* Рекомендуемая конфигурация RAID6+1HS. При необходимости могут применяться массивы RAID 10, RAID 50, RAID 60 аналогично HDD для обеспечения повышенной производительности в соответствии с проектными решениями.</p> <p>** Количество дисков в горячем резерве может быть увеличено в соответствии с проектными решениями.</p> <p>*** Применять RAID 6 HDD только для хранения архивных событий ПК. Для событий в оперативном доступе необходимо использовать HDD RAID 10.</p> |                                  |                                           |                               |                             |

Порядок подключения, отключения и эксплуатации определяется в документации, поставляемой совместно с оборудованием определенного типа в виде системы либо устройства хранения.

## Приложение Д

### Установка модулей сбора и обработки данных и модули выявления нарушений ИБ (корреляционной обработки данных)

**Примечание.** Номер версии дополнительных коннекторов Ankey SIEM NG и пакетов контента Ankey SIEM NG имеет формат A.B.C, где А – минимально поддерживаемая версия платформы ПК Ankey SIEM NG, В – мажорная версия изделия, С – минорная версия изделия. Например: 5.1.0.

Для определения версии установленного коннектора и контента см. документ «Руководство администратора Ankey SIEM NG 5.2.3», разделы «Версия дополнительного коннектора» и «Версия пакета контента».

#### Д.1 Установка дополнительных модулей сбора и обработки данных

Модули сбора и обработки данных (далее также – коннекторы Ankey SIEM NG) предназначены для интеграции ПК Ankey SIEM NG с источниками событий.

Посредством коннекторов обеспечивается предварительная обработка событий на сервере обработки Ankey SIEM NG Server с помощью правил нормализации. Предварительная обработка осуществляется в целях приведения структуры событий источников к единому формату ПК Ankey SIEM NG. Правила нормализации выполняют первичную обработку событий (парсинг, маппинг) и категоризацию (обогащение сведений категориями для последующей корреляционной и аналитической обработки). После обработки события передаются в сервер хранения Ankey SIEM NG Storage.

В ПК Ankey SIEM NG предусмотрены следующие типы коннекторов:

- **стандартные коннекторы**, которые входят в комплект поставки ПК Ankey SIEM NG и предназначены для интеграции ПК Ankey SIEM NG со стандартными источниками событий<sup>36</sup>.  
Установка стандартных коннекторов Ankey SIEM NG описана в подразделе 3.14 этого документа.
- **дополнительные коннекторы**, предназначенные для интеграции ПК Ankey SIEM NG с нестандартными источниками событий<sup>36</sup>, которые не поставляются с платформой ПК Ankey SIEM NG по умолчанию (не являются «коробочным» решением).

<sup>36</sup> Списки поддерживаемых стандартных и нестандартных источников приведены в приложении к документу «Руководство по интеграции с источниками событий Ankey SIEM NG 5.2.3».

**Внимание!** Вся детализация и особенности установки и настройки сбора событий от нестандартных источников в ПК Ankey SIEM NG описана в документации на использование дополнительных коннекторов, которая поставляется в рамках приобретения таких изделий.

❖ Основной алгоритм установки дополнительного коннектора в Ankey SIEM NG следующий:

1. Импортировать в систему файл дополнительного коннектора Ankey SIEM NG.
2. Выполнить установку коннектора в Ankey SIEM NG Server.
3. Выполнить настройку профиля Ankey SIEM NG для сбора событий с источника.
4. Создать и запустить задачу для сбора событий.

## Д.2 Установка дополнительных модулей выявления нарушений ИБ (корреляционной обработки данных)

Модули выявления нарушений ИБ (корреляционной обработки данных) (далее также – контент Ankey SIEM NG) – это набор взаимосвязанных инструментов ПК Ankey SIEM NG (правила обогащения, правила агрегации, правила локализации, правила корреляции, макросы и табличные списки), предназначенный для автоматизации процесса предупреждения, обнаружения и реагирования на инциденты ИБ.

В ПК Ankey SIEM NG предусмотрены следующие пакеты контента:

1. Стандартные пакеты контента, которые входят в комплект поставки ПК Ankey SIEM NG:
  - **пакет общих ресурсов контента (ПОРК)** – коробочный набор ресурсов для корреляции и анализа данных, содержит общие макросы, общие табличные списки, общие правила обогащения и набор корреляционных правил для всех типов источников, необходимых для работы верхнеуровневых пакетов контента;

**Внимание!** Установка пакета общих ресурсов контента Ankey SIEM NG описана в разделе 3.14. Настройка пакета общих ресурсов контента описана в документе «Пакет общих ресурсов контента <Номер версии пакета>. Описание».

- **пакет мониторинга SIEM** – наборы инструментов мониторинга и выявления инцидентов для автоматизации процесса обнаружения подозрений на инциденты ИБ. Пакет функционирует на событиях внутреннего аудита ПК Ankey SIEM NG и предназначен для выявления

воздействия на ключевые ресурсы платформы со стороны пользователей и системы.

2. Дополнительные пакеты контента (не являются «коробочным» решением):
  - **инфраструктурный пакет контента (ПИК)** – наборы инструментов мониторинга и выявления инцидентов для различных типов источников;
  - **пакет мониторинга ПО SCADA (SCADA)** – наборы инструментов мониторинга и выявления инцидентов для источников событий типа АСУ ТП;
  - **пакет мониторинга SOC (SOC)** – наборы инструментов мониторинга и выявления инцидентов для выявления распределенных атак на различные дочерние общества, функционирует на верхнем уровне иерархии ПК Ankey SIEM NG;
  - **пакет обнаружения компьютерных атак. Корпоративный сегмент (ПОКА КС)** – наборы инструментов мониторинга и выявления инцидентов, которые предназначены для выявления вредоносной активности в инфраструктуре на основе матрицы MITRE ATT&CK, а также для последующего построения цепочек атак и их обогащения в случае распределенного во времени развития атаки.

## Д.2.1 Иерархия пакетов контента

Пакеты контента Ankey SIEM NG имеют иерархию, от которой зависит порядок наследования правил:

- Уровень 4 (верхний) – SOC;
- Уровень 3 – SCADA, ПОКА КС;
- Уровень 2 – ПИК, SIEM мониторинг;
- Уровень 1 (нижний) – ПОРК.

Каждый пакет контента может использовать свои ресурсы, а также ресурсы пакета, расположенного ниже его в иерархии пакетов в KB. Например, пакет верхнего (4го) уровня может ссылаться на ресурсы пакетов 3го, 2го или базового уровня. Пакет 2го уровня может использовать ресурсы пакета базового уровня, но не может использовать ресурсы 3 и 4 уровня. Пакет базового уровня может использовать только свои ресурсы.

Для корректной работы ресурсов необходимо соблюдать иерархию пакетов при установке пакетов в KB. Первым необходимо устанавливать пакет базового (1го) уровня, затем пакеты 2го, 3го уровня и в конце – пакет верхнего уровня.

## Д.2.2 Установка и удаление дополнительного пакета контента в ПК Ankey SIEM NG

После создания корневой базы данных и пользовательской ветки, создание которых представлено в разделе 3.14, пункт **Пакеты экспертизы** раздела **SIEM** приложения **Knowledge Base** примет вид<sup>37</sup>, представленный на рисунке Д.1.

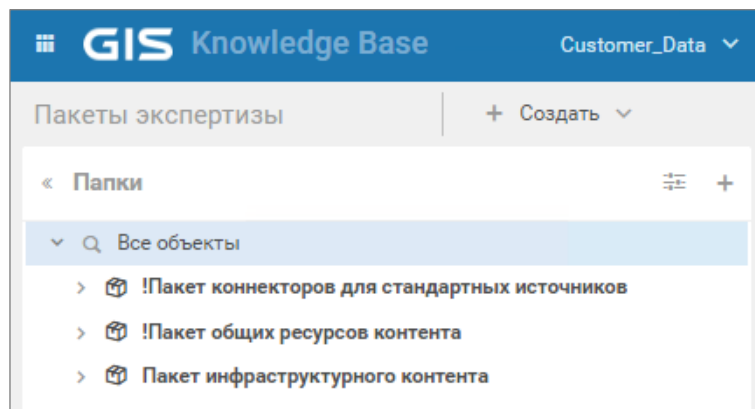


Рисунок Д.1 – Облик пользовательской ветки Customer\_Data

Для нормализации и последующей корреляции событий, объекты Knowledge Base необходимо:

- валидировать;
- установить в SIEM.

Объекты Knowledge Base не задействуются в процессах нормализации и корреляции событий автоматически. Для применения правил к потоку событий с источников необходимо произвести их установку в SIEM. О том, что объект не установлен в SIEM, свидетельствует красный значок  или его отсутствие.

Пример не валидированного и не установленного в конвейер объекта приведен на рисунке Д.2.

<sup>37</sup> Состав пакетов может отличаться.

|                                                                                                                                                                                                                  |                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Правило предназначено для обнаружения событий удаления файлов, которые запрещены к удалению. Табличный список конфигурации: "COMMON_Files_Forbidden". Табличный список исключений: "COMMON_Tracking_Exceptions". |                                                                                        |
| Системное название                                                                                                                                                                                               | TTS_35_Deleting_Files_Prohibited_For_Deletion                                          |
| Идентификатор                                                                                                                                                                                                    | GIS-CR-100800193                                                                       |
| Тип                                                                                                                                                                                                              | Стандартный                                                                            |
| Поставщик                                                                                                                                                                                                        | GIS                                                                                    |
| Папка                                                                                                                                                                                                            | !Пакет общих ресурсов контента/Правила корреляции/Подмена или фальсификация информации |
| Наборы для установки                                                                                                                                                                                             | Актуальный набор ресурсов SIEM                                                         |
| Статус валидации                                                                                                                                                                                                 | !                                                                                      |
| Статус установки                                                                                                                                                                                                 | ↓                                                                                      |

| №... | С... | Идентификатор    | Системное название                            | Описание                                              | Тип         | ↓ |
|------|------|------------------|-----------------------------------------------|-------------------------------------------------------|-------------|---|
| 1    | !    | GIS-CR-100800193 | TTS_35_Deleting_Files_Prohibited_For_Deletion | Правило предназначено для обнаружения событий удал... | Стандартный | ↓ |

Рисунок Д.2 – Пример не установленного и не валидированного объекта

### Валидация ресурсов Knowledge Base

**Валидация** – это проверка объекта на предмет соответствия синтаксису языка XPR, а также наличия всех необходимых зависимостей от других ресурсов (например, табличных списков и макросов). О том, что объект не валидирован, свидетельствует значок !.

❖ Для валидации объектов необходимо выполнить следующие действия:

1. В правом верхнем углу на панели инструментов выбрать инструмент **Валидация**, как показано на рисунке Д.3.

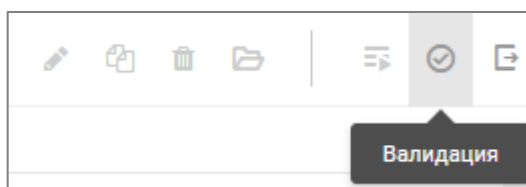


Рисунок Д.3 – Инструмент Валидация

2. В открывшемся окне выбрать **Все объекты** или **<объекты из набора для установки>**<sup>38</sup>, или **<название\_объекта>** и

<sup>38</sup> Процесс создания наборов для установки подробно описан в документе «Руководство оператора Ankey SIEM NG 5.2.3» в разделе «Работа с наборами для установки».

запустить процесс валидации нажатием кнопки **Запустить валидацию**.

- После успешного завершения процесса, статус валидации всех объектов изменится. О том, что объект валидирован, свидетельствует значок .

### Установка ресурсов в Ankey SIEM NG Server

Для установки объектов в конвейер необходимо выполнить следующие действия:

- В главном меню в разделе **<Название базы данных>** выбрать ветку **Customer\_Data**, созданную в разделе 3.14.5.
- В главном меню в разделе **SIEM** выбрать **Пакеты экспертизы**. Откроется страница **Пакеты экспертизы**.
- Если набор для установки создавался ранее, перейти к п.10. Если набор для установки не требуется, то нужно выбрать набор «Все объекты» и перейти к п.16.
- В панели **Наборы для установки** внизу слева нажать **+**. Откроется окно **Создание набора для установки**<sup>39</sup> (рисунок 3.21).

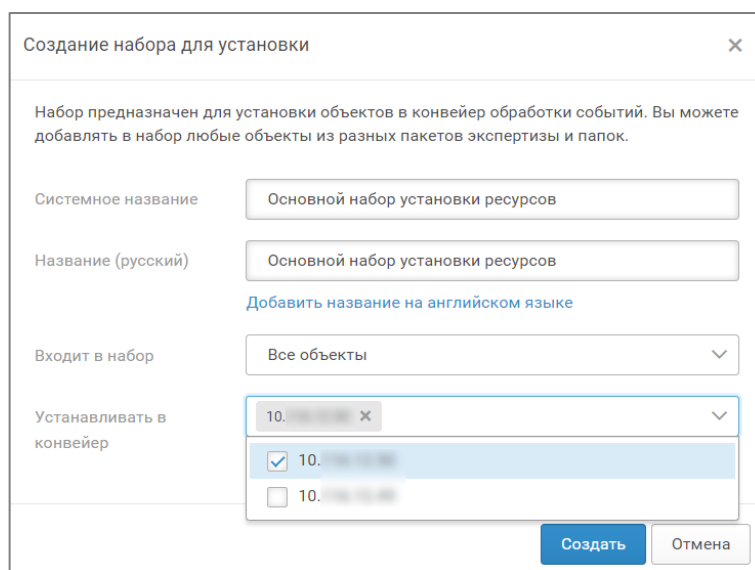


Рисунок 6.1 – Создание набора для установки

- В поле **Системное название** ввести название набора. Рекомендуется указать системное название на латинице.
- В поле **Название (русский)** возможно внести любое значение, оно будет отображаться в веб-интерфейсе. Например, «Набор для ресурсов аминистрации»

<sup>39</sup> Подробно о наборах для установки в документе «Руководство оператора», раздел «Работа с наборами для установки»

7. В поле **Входит в набор** выбрать **Все объекты** или любой другой корректно сформированный набор для установки.
8. В поле **Устанавливать в конвейер** выбрать один или несколько конвейеров, в который будут установлены ресурсы из набора установки.  
Выбрать конвейеры для установки возможно только в том случае, если корректно выполнена установка всех основных компонентов ПК Ankey SIEM NG.

**Внимание!** На главном конвейере<sup>40</sup> должны быть установлены все правила, которые есть на дополнительных конвейерах. Несоблюдение этого требования вызовет некорректную работу правил локализации. В случае установки коннектора не на главном конвейере, а только на целевом, необходимо продублировать пакеты ресурсов в главный конвейер.

9. Нажмите кнопку **Создать**.  
Набор для установки создан.
10. В панели **Наборы для установки** выберите **Все объекты**.
11. В панели **Папки** выберите необходимый пакет экспертизы (или папку).  
Появится список объектов пакета экспертизы (папки).
12. Выберите необходимые объекты.

**Примечание.** Содержимое набора для установки следует формировать с учетом того, что при установке новых ресурсов в компонент Server ресурсы, которые были установлены ранее, автоматически и принудительно удаляются, а новые устанавливаются.  
Поэтому набор для установки должен содержать полный набор необходимых правил нормализации, корреляции, обогащения, агрегации и табличных списков без учета установленных ранее ресурсов.

**Внимание!** В случае использования схемы «горизонтальный SIEM» при установке ресурсов в конвейеры необходимо всегда добавлять в набор установки следующие табличные списки из пакета общих ресурсов контента:

- COMMON\_Tracking\_Exceptions
- COMMON\_Hosts\_Configuration
- COMMON\_Users\_Configuring
- COMMON\_Files\_Forbidden
- COMMON\_Hosts\_Scada\_Zone
- COMMON\_VIRT\_Critical\_VM

Если это условие не будет выполнено, установка ресурсов завершится ошибкой.

<sup>40</sup> Проверить, является ли конвейер главным, можно в приложении Ankey SIEM NG → Система → Управление системой → Конвейеры на боковой панели справа.

13. Нажмите на графическую кнопку  .  
Откроется окно **Наборы для установки**.
14. Установите флажок напротив названия набора для установки, в который нужно добавить объекты.
15. Нажмите кнопку **Сохранить**.  
Объекты добавлены в набор для установки.
16. Из набора установки необходимо удалить все родительские ресурсы, с которых были созданы копии в ветке **Customer\_Data**, чтобы не было конфликтов в работе SIEM-системы после установки. Найти родительский ресурс, выделив скопированный, возможно, перейдя к нему по ссылке из описания скопированного ресурса в панели справа, как показано на рисунке

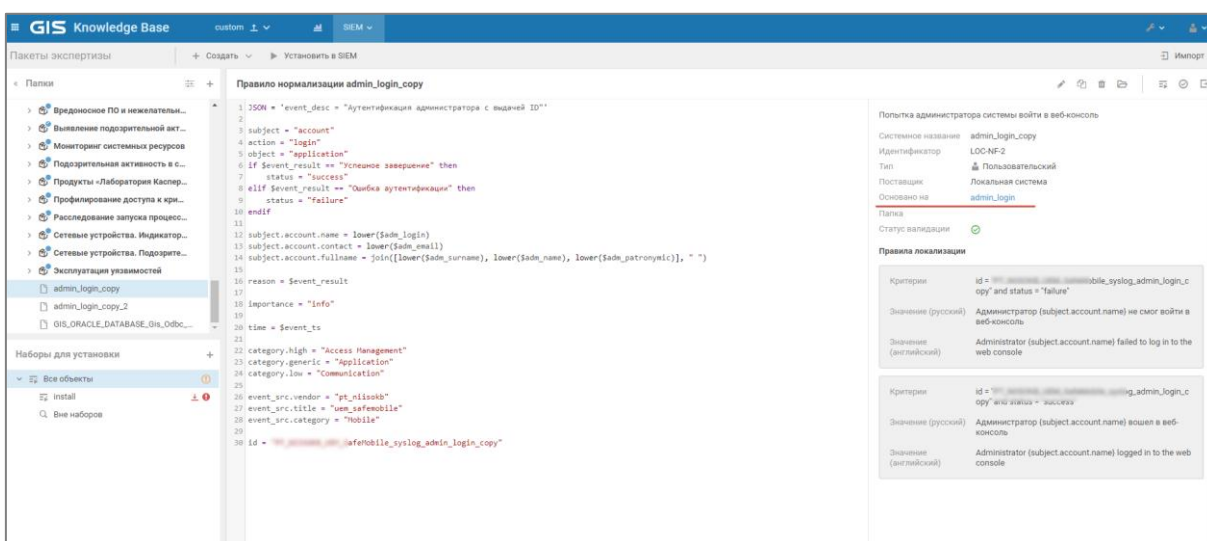


Рисунок 6.2 – Ссылка на родительский ресурс

17. В верхней части страницы на панели инструментов выбрать инструмент **Установить в SIEM**, как показано на рисунке Д.4.



Рисунок Д.4 – Инструмент Установить в SIEM

18. В открывшемся окне отметить необходимый конвейер и запустить процесс установки нажатием кнопки **Запустить установку**, как показано на рисунке Д.5

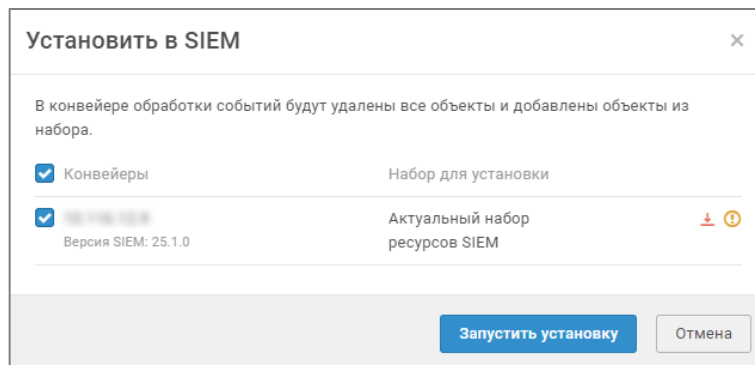


Рисунок Д.5 – Окно установки объектов в конвейер

19. После успешного завершения процесса, статус установки объектов изменится. О том, что объект установлен в конвейер, свидетельствует значок .

**Внимание!** При выполнении указанных действий для объектов из набора для установки валидации и установке подвергается именно состав ресурсов в наборе. В случае ошибок, связанных с отсутствием необходимых объектов, следует убедиться, что в наборе для установки учтены все зависимости между ресурсами.

### Удаление из конвейера

❖ Для удаления объектов из конвейера необходимо выполнить следующие действия:

1. Выбрать необходимые ресурсы и в правом верхнем углу на панели инструментов выбрать инструмент **Наборы для установки**, как показано на рисунке Д.6.

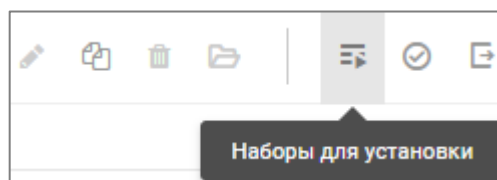


Рисунок Д.6 – Инструмент Наборы для установки

2. В открывшемся окне снять галочку принадлежности к набору для установки, который привязан к конвейеру, из которого следует удалить объекты, как показано на рисунке Д.7.

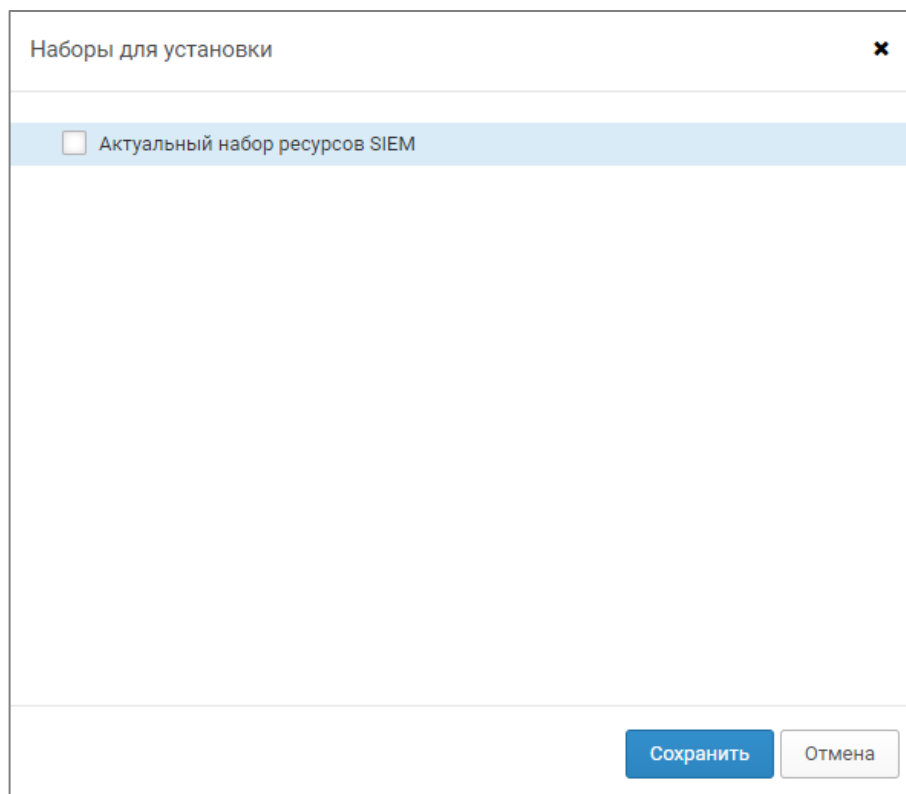


Рисунок Д.7 – Окно выбора наборов для установки

3. Установить объекты в конвейер, как было описано ранее.

**Внимание!** Удаление из конвейера не подразумевает удаление объектов из Knowledge Base.

### Д.2.3 Работа с ресурсами в пользовательской ветке Customer\_Data

Пользовательская ветка Customer\_Data подразумевает наличие в ней стандартных (эталонных) копий объектов, которые недоступны для редактирования и удаления. Но в ходе эксплуатации ПК Ankey SIEM NG может потребоваться изменить параметры правил, например, пороговые значения срабатываний правил корреляции, заполнение полей правил нормализации или тексты правил локализации.

Модификация стандартных объектов может быть выполнена только посредством копирования объекта. При копировании новый объект появляется в Knowledge Base как пользовательский и доступен для дальнейшего редактирования и удаления.

**Внимание!** На модифицированные пользователем ресурсы пакетов экспертизы не распространяется техническая поддержка.

После копирования объекта необходимо учитывать, что наличие двух идентичных по логике работы правил, установленных в SIEM, приведет к ложным

срабатываниям, поэтому оригинальный объект, на основе которого делалась копия, должен быть удален из SIEM, а новый, скопированный, установлен в соответствии с инструкцией, приведенной в разделе Д.2.2.

Ограничения на создание новых объектов в пользовательской ветке отсутствуют.

**Внимание!** Создание новых объектов в эталонной корневой базе данных **GIS\_DB** запрещено!

Процесс работы с ресурсами подробно описан в документе «Руководство оператора Ankey SIEM NG 5.2.3».

## Приложение Е

### Применение патчей в ПК Ankey SIEM NG (5.2.3)

После установки основных компонентов ПК Ankey SIEM NG необходимо ознакомиться с данным разделом и проверить наличие пакетов исправлений (патчей) в текущей версии Системы. Пакеты исправлений включены в дистрибутив ПК Ankey SIEM NG и предназначены для исправления некритичных ошибок текущей версии Системы.

В случае наличия пакетов исправлений, необходимо перейти в папку, содержащую пакет исправлений и выполнить шаги, приведенные в инструкции в формате TXT, которая находится в папке с пакетом исправления.

Пакеты исправлений находятся по пути < Ankey SIEM NG 5.x.x SR (26.x.xxxxx) >/<Дополнительно> в составе дистрибутива ПК Ankey SIEM NG.

В версии ПК Ankey SIEM NG 5.2.3 (26.2.13166) были добавлены следующие исправления:

- 1. Патч для устранения уязвимости обхода аутентификации в Ankey SIEM NG MC**  
Данный патч устраняет уязвимость, при использовании которой возможно обойти аутентификацию в Ankey SIEM NG версии 5.2.3 SR (26.2.13166). В случае успешной эксплуатации уязвимости возможно имперсонировать любую учетную запись Ankey SIEM NG MC и получить все возможные привилегии.
- 2. Патч для исправления бесконечной перезагрузки службы Topology**  
Данный патч исправляет бесконечную перезагрузку службы Topology после обновления Ankey SIEM NG с версии 4.1 SR (25.1.5988) до версии 5.2.3 SR (26.2.13166).
- 3. Патч для исправления проблем с репликацией событий по иерархии**  
Данный патч исправляет рассинхронизацию событий между площадками в иерархии и решает проблему неправильной сериализации даты при отправке в ресивер.
- 4. Патч для исправления проблемы с задачей проверки событий на наличие IOC**  
Данный патч устраняет ошибку при использовании профиля IOC search for hash в задачах проверки событий на наличие в них идентификаторов компрометации (IOC) в Ankey SIEM NG версии 5.2.3 SR (26.2.13166).
- 5. Патч для исправления ошибки при аудите ОС Windows**  
Данный патч устраняет ошибку при использовании доменной учетной записи для аудита операционных систем семейства Windows в Ankey SIEM NG 5.2.3 SR (26.2.13166) с помощью компонента Ankey SIEM NG Collector для ОС Linux.
- 6. Патч для исправления повторного сбора событий ОС Windows коллектором в ОС Linux**  
Данный патч исправляет повторный сбор событий ОС Windows коллектором в ОС Linux в Ankey SIEM NG 5.2.3 SR (26.2.13166).